DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Information Systems

Analyzing the Influence of Chinese Data Protection Regulations on Foreign Companies Operating in China: An Empirical Study

Lukas Vester and Vinicius Agreste

DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Bachelor's Thesis in Information Systems

Analyzing the Influence of Chinese Data Protection Regulations on Foreign Companies Operating in China: An Empirical Study

Analyse des Einflusses der chinesischen Datenschutzvorschriften auf in China tätige ausländische Unternehmen: Eine empirische Studie

Author:	Lukas Vester and Vinicius Agreste
Supervisor:	Mo Chen
Advisor:	Professor Jens Großklags
Submission Date:	15.07.2024

We hereby confirm that this bachelor's thesis in information systems is our own work, and we have documented all sources and material used.

Wir versichern hiermit, dass wir die von uns eingereichte Bachelor Arbeit in Wirtschafsinformatik selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt haben.

Both researchers were actively involved in every stage of the process, encompassing data collection, identifying and recruiting interviewees, preparing and conducting interviews, analyzing the gathered data, and documenting all findings in this thesis.

Munich, 15.07.2024 Lukas Vester and Vinicius Agreste

Acknowledgments

We want to thank our advisor, Mo Chen Ph.D., for her support and orientation throughout the development of this work. We thank our supervisor, Prof. Dr. Jens Grossklags, for his guidance. We also appreciate all industry members who agreed to contribute to our research. Thank you for sharing your time and knowledge in our surveys and interviews.

Abstract

The 2021 Chinese Personal Information Protection Law (PIPL) defined regulatory terms for all firms handling data originating in China. In combination with the other two data-related regulations in effect, the Data Security Law (DSL) and the Cybersecurity Law (CSL), China has taken another step in securing its cyberspace.

As with the European General Data Protection Regulation (GDPR), the regulations aim to bring significant changes and establish new requirements for personal data collection, processing, access, transfer, and rights for natural persons. Given their extraterritorial scope, the effect of said regulations on foreign companies could be substantial. Still, there has been little empirical research on the topic. By interviewing multiple international companies operating in China, we aim to assess the extent to which foreign companies have been affected by these regulations and how they have responded.

We conducted 20 interviews and collected five survey responses from participants in nine industry segments with various knowledge levels. We observed that although many industry members consider the laws to be vague and a source of uncertainty, some, relying on regulatory knowledge, held positive positions on the subject. After combining our results with insights from the literature, we believe that an exaggerated depiction of enforcement activities and intentions by Chinese authorities in various publications can be a moving factor in increasing reluctance in the market.

Furthermore, conflicting contributions regarding enforcement activities and general impressions of the regulations were noted. Whilst attempting to investigate these findings, the research team observed that certain groups were more significantly affected, which correlated to how the regulations were perceived. Our findings propose that the following groups require special attention when navigating the Chinese cyberspace: service providers that require low latency from servers, big data handlers, businesses located at the end of the supply chain (assemblers), enterprises operating in sensitive industries, and Small and medium-sized enterprises (SMEs) attempting to penetrate the market. Differences in perceived enforcement strictness, based on location, revealed that regional authorities could be another potential explanation for the conflicting opinions.

Our results show that data localization and effective resource management are firms' most affected operational activities. Strategic planning allied with investments in up-to-date information or professional consulting are the most effective measures for foreign firms in China. Further research must be conducted after the regulations were flexibilized in March 2024 to challenge these findings.

Contents

1 Introduction

The importance of China for the global economy has long become unquestionable. After opening to reforms in 1979, China's annual real GDP averaged 9.5% until 2018 [1]. In 45 years, China's GDP went from 11% of the US level [2] to 70% [3]. It is no wonder that, given the country's economic relevance, every new law, regulation, or taxation that impacts the Chinese market reverberates to the whole world's economy. The consequences of internal decisions are not limited to the Chinese territory or companies alone and said consequences become even more significant when the changes in question refer to topics present in multiple economic sectors, such as personal data. In such conditions, the PIPL, CSL, and DSL regulations come into effect; hence, there is a need to research their potential impact.

In August 2021, China passed the Personal Information Protection Law (PIPL), a set of regulations regarding Chinese personal information, following similar regulations as the European Global Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA) [4]. The PIPL's goal is to grant protection and privacy to all residents in China regarding their personal information on the internet. This includes granting rights protected by the GDPR, such as the "Right to be Informed" - to know the intent behind the collection of data -, the "Right to Erasure" - protects the right to request an organization to erase any data related to the subject -, and the "Right to Rectification" - to be able to correct or complete inaccurate data [5, 6]. Furthermore, the regulation's scope is extraterritorial, so its jurisdiction includes companies or other agents outside of China that process data from individuals within China [7, 8]. Therefore, Chinese and foreign entities operating in China are subject to the mentioned legislation.

The relatively recent introduction of the PIPL is the next step in the country's effort to regulate its cyberspace, adding yet another regulation along with the Cybersecurity Law of the People's Republic of China (CSL, commenced in November 2017) and the Data Security Law of the People's Republic of China (DSL, effective September 2021) [9]. There is considerable legal overlap between the regulations; however, each has a specific purpose. The CSL establishes the general security framework, for instance, the requirements for collecting, using, and protecting personal information. While the DSL regulates the handling of processed data, ensuring data security [10].

The combination of said regulations has created a thick mesh of laws that external firms must navigate to keep operating in Chinese digital territory. Multiple analytical and descriptive works have been created by legal or consulting firms, data protection authorities, and business professionals. However, there is a decisive lack of empirical research conducted on the effect

of these regulations on non-Chinese firms, which has prompted us to investigate the situation objectively. Our research aims to understand the industry's response to the new regulations. That includes companies' outlook on the subject, adopted measures, current compliance levels, and planned changes in business models and operations in and out of China.

The first step in our experimental methodology was to gather information and increase our knowledge base on the subject. We summarized and structured our findings to refine our understanding as well as identify any potential gaps in our comprehension. The next step was crucial and involved collecting data via interviews with industry players. In total, 20 interviews were conducted across seven industries (Consulting, Healthcare, Real Estate, IT, Law Firm, Engineering/Manufacturing, and Public Trade), producing around nine hundred minutes of recordings, later transcribed into 167 pages of text. After processing the collected results, we conducted a structured coding process on the interviewees' responses. We categorized and identified patterns to transform the collected qualitative data into quantitative data for analysis, producing more than three hundred entries. Lastly, the data was analyzed, and we extracted all useful information, ultimately enabling us to conclude how different entities have been or will be affected by the new regulations and evaluate if theoretical publications are aligned with practice.

Concerning this thesis' structure, this brief introduction is followed by a literature review, where the articles and publications that built the foundations of our understanding of the topic will be summarized. Then, we will briefly cover our initial predictions and thoughts. The following section covers our research method: how the research data was gathered, structured, and ultimately, analyzed. Section five displays the interview's qualitative results, followed by their examination in section six, and finally, in the seventh and last section, we showcase this research's conclusion. Additional resources in the appendix include our email templates, interviewed companies overview, and the link to a GitHub repository containing interview scripts and coding results.

2 Literature Review

Multiple works aided our understanding of the set of laws and their possible effects. As previously stated, few articles empirically analyzed the new regulation's potential impact on national or global companies. However, multiple works on the subject approached the discussion from the legal and business sides, summarizing the regulation's most impactful measures, limitations, requirements, and possible changes and necessary countermeasures for affected international companies. Furthermore, a clear comparison between these and similar regulations under other national legislations across the globe was also highly insightful.

In Yvonne Lau's article [11], she lays down some foundational concepts necessary to understand the legislation entirely. Firstly, the motivation behind the regulations relates to China's late arrival to the race of national powers attempting to control and protect their data spaces. The PIPL has been compared extensively with other personal data protection laws, such as the CCPA and the European GDPR. Next, the author describes the basic operational procedure of Chinese regulations: companies collecting, processing, analyzing, or using data in China are banned from transferring said data abroad without previous approval from an authority. However, as stated by Lau, besides being possibly subject to a fine if not compliant, "*the law does not outline how companies should obtain this approval or which agency they should approach to do so*."

On the one hand, the regulations intend to define individual rights in the data space, but on the other, they boost the Chinese government's control over once privately owned data. This is illustrated under yet another requirement of the regulation, the "data classification protection system," which defines that data should be categorized into, as of currently, "important" (data directly related to or that could identify an individual), "controlled items" (data with controlled exportation), or of "national security" (data that could represent a threat to national interests and security) (Article 51, PIPL [9]). The issue is that the definitions of all categories are broadly defined, leaving much room for interpretation by the judging authorities. Not to mention that, except explicitly for the automotive industry, the definition of "important data" must still be narrowed down for each sector.

The brief [12] written by Samm Sacks and Manyi Kathy Li, published at the Center for Strategic & International Studies (CSIS), summarized the contents of the PIPL and strategic intentions behind its design, for instance, the vagueness with which some requirements are established. According to the authors, obscurity could be leveraged to ensure flexibility in the government's position and make the enforcement situational. Furthermore, the authors raise an important point for our research, namely how the system could be used to punish foreign

companies and favor national ones for two main reasons. Firstly, amid vaguely defined cybersecurity standards, international companies would have to adapt their products and services to the Chinese market, perhaps constantly, as new requirements emerge. While Chinese firms are not excluded from this difficulty, there is no need for re-adaptation of their products or services since they are designed for the Chinese market in the first place. Not to mention that these companies are less preoccupied (in comparison to external firms) about sharing sensitive data with law enforcement authorities since their data is already locally stored and can be accessed. Secondly, foreign companies can be perceived as less trustworthy, in other words, with greater room for security concerns, as China "*suspects of foreign technology, regardless of whether it is true*" [13]. The consequences of said suspicion for international companies could be longer waiting times for approval by local authorities, more significant product redesign costs, and higher bureaucratic efforts in communication with law officials.

Matt Haldane's South China Morning Post article [14] depicts the reaching limits of the three laws in effect. By first describing the first case of a cybersecurity review on a private company, the tech mobility giant Didi Chuxing [15], the Haldane contends that Beijing is actively advancing its pursuit of a "cyber sovereignty" policy. Haldane describes some measures companies must comply with to continue operating in Chinese cyberspace: "Place someone in charge of cybersecurity, conduct training, and classify, backup, and encrypt important data" [14]. The author then elaborates on the regulation's scope, describing its extraterritorial character and its power to limit data transfer. The first aspect refers to the fact that the regulations are applied to data processed within and outside China as long as they "*harm the national security, the public interests, or the lawful interests of citizens or organizations*" [16] of China. The second aspect touches upon two newly added rules to companies handling what is considered "critical information," namely, that they must store said data within Chinese territory and that they must receive a regulating entity's approval after a security assessment to ship said data overseas, as stated by the author. Furthermore, the work mentions that violations of said rules could result in multiple kinds of punishment. Important data leaked or transferred irregularly could generate fines of from one hundred thousand upwards to one million yuan, with regulating authorities possessing the protected right to apply fines to individuals in charge of cybersecurity. Other penalties include suspension of business services, license revocation, and general civil and criminal liability.

Although the laws came into effect in 2021, there have been few public cases of individuals being personally guilty of an infraction. It was, however, the case for a businessman mentioned in The Economist's article, "China's data-security laws Rattle Western Business Executives" [17]. The individual in question, who was charged for illegal usage of "private information" of Chinese individuals, only came to know of said charges when landing in Singapore whilst on a business trip. This illustrates the uncertainty and strictness of the laws. The article refers to a lawyer who states, "*The Personal Information Protection Law of 2021 is one of the strictest such statutes in the world*," with another referenced law professional stating that, "*Merely forwarding an email with a signature containing a Chinese citizen's personal information*

may constitute an infraction,". Amidst the apparent strict nature of the law, the author states that the vast majority of international companies in China are still not compliant and have formally pleaded with local authorities for a deadline extension to ensure compliance. This article reassured the need for empirical study on the subject. An academic assessment of the company's compliance status concerning the law's requirements would enhance the global perspective on the data protection laws' impact and compliance processes. Furthermore, an empirical study could examine claims such as the article's conclusion: "*To fully comply, corporations will probably need to turn their China businesses into islands of information that have little contact with their global operations,*" Therefore, assessing said risk for business decisions has never been more crucial. Our study could provide companies or researchers with an empirical perspective from active members in China.

With a much more solid understanding of the PIPL, DSL, and CSL, we came across works from industry-leading consulting firms that explored these regulations and their newly set requirements for companies operating in China. These articles enlightened our understanding of concrete actions that companies are taking to stay compliant with regulations. "How China's data privacy and security rules could impact your business" [18], by Chi Chen and Leo Zhao, reinforces the need for company self-assessment regarding "compliance maturity," including those with high data privacy standards. Under the firm's offered services on information governance and privacy services, Chen and Zao highlight the capacity to identify non-compliant topics through a region-specialized team and analyze current data processing behavior. Furthermore, they promise to bridge the gap between as-is and to-be requirement compliance by employing dedicated sector professionals who assist clients in adapting their non-compliant processes. Another crucial report was PwC's "10 ways China's new data rules will change your business" [19]. It emphasizes the vast cost changes that the PIPL could potentially represent for companies with large operations in China, but mainly those inserted in the markets designated by China as highly sensitive, for instance, technology, retail, automotive, banking, and pharmaceutics. In addition to that, it also sheds light on actionable items for companies, for instance, reorganizing information systems to store data in China, reevaluation of previous investments or deals based on cost changes, updating legal and tax strategies to adapt to new practices, and law requirements, and evaluate vendors and supply chains to assess risk. Lastly, the article mentions that all actions in this space are an effort to mitigate risk so that participation in the market is still valuable from a financial perspective. Our empirical research should inquire to what degree companies have implemented such (or other) actions and how confident they are with continuing operating in the market.

3 Predictions

In this subsection, we will present our general predictions prior to the interview process. Said predictions were mostly derived from vast contact with research materials, as elaborated in the literature review section, but also include expectations towards sourcing and interviewing processes.

The mention of said predictions is important for two main reasons. The first is the examination of theory-based statements by comparison with interviewee claims. Assessing if publications' predictions hold in practice has been one of the goals of this research. Furthermore, by explicitly enumerating our predictions, we could identify and avoid bias in our research efforts. We were motivated to examine if industry members could, besides confirm or reject, expand the claims in our research materials. However, after having excessive contact with common trends in research material, there was a risk of limiting interviewees' contributions to topics mentioned in the literature. Listing our predictions was a useful guideline for identifying our biases when formulating research questions, as policy analysis should not blind us to new information. For reference simplicity, the predictions will be organized by topic and identified by a tag, as in <PX - Topic>.

Sourcing Process

SP1 - Response rate to emails (or other) inquiries will be low (5-10%), especially for companies that might not yet be completely compliant.

SP2 - Sourcing companies will be difficult, as data compliance can be considered sensitive information to share. Few companies will feel confident in sharing it.

SP3 - Individual employees may feel they lack permission to participate in an interview as a company representative.

Interviewing Process

IP1 - The validity of certain statements may need to be scrutinized further for all companies that choose to stay anonymous (fewer repercussions/traces for lying).

Regulation Impressions

RI1 - Companies will be skeptical about future operations in China.

Compliance Status

CS1 - Very few companies will directly admit to not implementing the new regulations, as it can result in potential backlash from China and the media.

CS2 - Companies that do not wish for anonymity will likely have implemented everything as required.

Enterprise Concerns

EC1 - Chinese authorities can abuse access to intellectual property or confidential information.

EC2 - Companies will feel overwhelmed by compliance rules, having to comply simultaneously with multiple data protection regulations worldwide.

EC3 - Security of employees, as authorities may hold individuals personally accountable for their company's non-compliant status.

Changes Caused

CC1 - Companies must rethink their investment strategies regarding existing and future projects in China.

CC2 - Financial burden, as new regulations, can be time-consuming as well as financially taxing.

CC3 - Companies are either planning a great restructuring within their Chinese sectors and services or are planning to shrink their participation in the market.

Parallel Regulations

P1 - Companies will find it more difficult or resource-consuming to adapt to the PIPL compared to the GDPR.

P2 - Companies will mention the lack of clearness in the PIPL compared to the GDPR.

4 Methodology

After diving deeper into the research topic and better understanding the regulations, it was time to plan our next steps. Our research aims to analyze companies that conduct business with China and determine how they adapt to the new Chinese data protection regulations. We aimed to approach our research question empirically, which required us to gather qualitative data. Said data should then be structured, coded into quantitative data, and ultimately analyzed to extract potentially valuable information. This section will address this process, including our setbacks and selected strategies.

4.1 Identifying Potential Issues

Before collecting data, we made initial predictions and brainstormed potential issues. We tried to consider as many factors as possible to minimize the chances of being surprised by an unforeseen variable in the future and took steps to address them. For instance, we noticed that relying on our personal networks as a sourcing method could pose a risk to representative results, as both researchers had similar academic backgrounds. We then made sure to expand our sourcing efforts beyond our networks. However, there were risks which we judged to be unavoidable. There was no guarantee of a specific amount of participants, given that participation was voluntary. As deep knowledge of the topic was not a prerequisite for participation, participants could also be mostly composed of non-experts, potentially misrepresenting the industry's perceptions of the topic. By dissecting each identified risk as either unavoidable or addressable, the research team could better plan the data collection process, which is the leading theme of the following subsections.

4.2 Gathering Data

The next step in our research was gathering data. Literature publications, articles, and reports were an important source of information. The heterogeneous sources of said publications, such as consulting firms [20, 10], newspapers [17], academia [21] and governmental organizations [22] increased data quality. In addition to the aforementioned publications, reading through the regulations' translations [9, 23, 24], was also important. This was how we acquired our initial understanding of the topic and gained the fundamental knowledge required to conduct interviews with active industry members, our second and most important data source, as it

was the focus of our empirically-focused research. The following paragraphs focus on the interview process.

4.3 Create Script

A guideline for our interviews was necessary to ensure a smooth interview flow and target specific information. Whilst working on the guideline, we aimed to focus the interview on specific topics whilst enabling our interviewees to provide additional, potentially novel information. This enabled us to be very flexible during our interviews and gave us an invisible layer of support we could rely on. We got regular and constant feedback from our advisor, Mo Chen, Ph.D., every step along the way. She helped us stay on track and avoid potential pitfalls. We were able to improve our interview script through multiple iterations with her and our professor, Prof. Dr. Jens Großklags. We added a backlog of potentially interesting questions that may not already have been indirectly covered in prior questions and would be used if enough time remained at the end of the interview. Our original script was in English, however, we also wanted to reduce the risk of a language barrier hindering participation. Thus, we also decided to hold interviews in German and consequently prepared a German translation of our script.

4.4 Email Templates

In parallel to developing our interview script, we started working on email templates 8.1 to standardize and accelerate sending out interview invitations. We paid close attention to avoid potential spam trigger expressions, such as "urgent" and "fast response," which could cause our email to be flagged as spam and automatically blocked. To make our email more trustworthy, we included a signed endorsement document from our professor and the Chair of Cyber Trust at the Technical University of Munich.

4.5 Sampling Method

At the same time as we were working on our script and email template, we also worked on collecting a list of potential interviewees. At this stage, we decided to utilize the convenience sampling method for gathering interviewees. This non-probabilistic sampling approach was selected because of its "*little effort, cost, time investment, and its simple operation*" [25].

Research on the method exposes some setbacks, such as the risk of bias, lack of representation for certain groups, and the inability to generalize results beyond the sample. However, said challenges might be mitigated by controlling for sample diversity and using external data [26]. Given the lack of empirical research available on this novel research topic, we were limited to theoretical publications (2). Extending our sampling beyond our network in order to reach a

more diverse group of potential interviewees was crucial to avoid the aforementioned risks. The exact methods with which we achieved said goal will be explored in the upcoming paragraphs.

4.6 Sourcing Process

We initialized the sourcing process by using the German Chambers of Commerce Abroad (Außenhandelskammer; AHK) Greater China's publicly available list of companies [27]. As AHK Greater China is part of the German Chambers of Commerce Worldwide Network, they were an excellent way to find relevant companies. Through their list, we acquired the names and websites of numerous German companies doing business in China and gathered more than 500 email addresses 5.1. Although this sourcing strategy resulted in a larger representation of German companies, potentially introducing bias, it also provided a clearer baseline for comparison. Our familiarity with the German market allowed us to better understand the adjustments the company needed to make in China.

Despite the promising large number of collected emails, the next step proved to be much more challenging than expected. After sending hundreds of emails, our response rates sadly were abysmal. Of our first one hundred emails, we received a total of two responses. One of which was a rejection whilst the other a confirmation. Initially, when we first began sending emails, we sent emails to any relevant addresses we could access. Over the course of the next several hundred emails, we never received any response from the generic email targets, such as "info@company.com" and the response rate from specific individuals ended up being in the low single percentages, even including rejections.

This made us aware of the kind of challenge we would be facing in order to obtain voluntary participants. Such a low response rate was a massive issue that we needed to tackle with extremely high priority. We spent numerous hours brainstorming potential reasons behind the low response rate and potential improvements in our strategy. One of our main concerns was that emails might not even arrive at the intended individuals and were blocked by company filters. With this in mind, we attempted to iterate over our email template in order to boost responses. We sometimes did not include the endorsement attachments, as we theorized attachments might trigger the filters. Furthermore, we created a second severely shorter version 8.2, as the main version might overwhelm a recipient because it contained well over five hundred words. We also optimized our templates by avoiding even more key phrases that might trigger any potential spam filters, even at the cost of providing less information. Many of the emails that were sent also contained very generic "Dear [company name] Team" greetings, which we tried to avoid when possible. This was, however, unavoidable in many cases, as many companies did not specify a particular contact person. This issue could be avoided when contacting individuals directly instead of companies generically. Furthermore, we also discovered that academic language is commonly used in spam emails to appear harmless. Thus, phrases such as "purely for academic purposes" and "participation is entirely voluntary" could have indirectly harmed us. Asking the potential interviewee to forward our

email could also have been seen as suspicious, as it is a common tactic used by spammers to spread their messages. As an alternative to a thirty-minute interview, we offered potential interviewees the option to complete a short survey containing our main questions.

As previously mentioned, generic company emails did not yield any positive results, so we turned our efforts to specifically target individuals. Thus, we heavily prioritized emails such as "firstname.lastname@company.com". We also diversified our sourcing strategy, expanding our search for contacts beyond the AHK company list [27] with a focus on gathering a more heterogeneous sample of companies. One new source of contacts ended up being the authors of relevant articles. Naturally, these authors were knowledgeable on the topic, but the mention of their professional contact information in the articles was particularly useful. By mentioning their articles in our contact email, we improved confidence levels and created a direct bridge to the potential interviewee, increasing response rates. Additionally, we also started attempting to contact potential interviewees via a popular networking platform. This method had a higher success rate and helped us secure many interviews. Furthermore, we went through our personal networks to contact potential interview candidates directly and acquire assistance in finding potential interviewees. The results of our sourcing process are depicted in Chapter Five in the 5.1 table.

4.7 Interviewing Process

After establishing initial contact, setting up interviews was simple. As we had two members capable of leading the interviews, arranging interview schedules was not an issue. As previously mentioned, whilst we did offer the option to do the interviews in German, we ended up only doing English ones. This had a couple of reasons. First of all, our knowledge of the proper technical terms is significantly higher in English, as we did all our prior research in English. Second, it ended up helping significantly in the later coding stages, making it substantially easier to standardize our collected data.

While conducting the interviews, we made sure to keep the participants anonymous. We never mentioned them or their company by name. Although we always had our standard script at hand, we made sure to go with the flow and keep track of time. Although we generally kept our interviews within thirty minutes, we occasionally had interviews where time was not an important factor, enabling the interviews to last longer than an hour. In most cases, we had two interviewers join every interview to mitigate any potential issues that might arise, given that all interviews were held online using programs such as Microsoft Teams and Zoom.

Each interview with two interviewers used the two roles of lead interviewer and observer. The lead interviewer would ask the questions and control the pacing, whilst the observer was responsible for taking notes and being prepared to step in in case any issues arose. An example would be, the main interviewer losing connection mid-interview due to internet issues. To mitigate the chances of data loss, both interviewers recorded the audio using two

independent methods of recording setup on different devices: QuickTimePlayer for Mac or Voice Recorder for Windows. Throughout our interviews, we encountered cases where our caution was rewarded, as we had case one of internet loss and two cases where devices were not able to record proper audio. One other significant issue we faced was when interviewees opted not to be recorded. This made documenting their responses significantly harder. In the cases where both interviewers were on the call, this issue could be mitigated by ensuring that both interviewers took notes. This, however, was not always the case, and sometimes useful information may have been lost.

With each interview, we improved our performance as interviewers, got better at guiding interviewees through our research questions, and extracted more insights from our exchanges. Our experience throughout the interview process showed that most of our predictions regarding the sourcing and interviews (3) were accurate.

4.8 Coding Process

We started interviewing companies in March of 2024 and were able to conclude them by June. After conducting the interviews and collecting vast amounts of qualitative data, the next step was to extract meaningful insights by performing "Qualitative Content Analysis" [28]. This process intends to extract meaning from qualitative data by simplifying, organizing, and structuring text data into categories and clusters. After these steps are taken, context, connections, and meaningful insights can be extracted more confidently.

There are, however, multiple techniques to do so. This article [28] describes three approaches to content analysis: conventional, direct, and summative. All approaches differentiate in advantages, disadvantages, and trustworthiness levels. However, the defining factors for our choice of the conventional strategy were: first, that coding categories are directly derived from the collected data, and second, that interviews can be structured to foster new contributions. The first relates deeply to our intent to lower the risks of imposing preconceived categories based on our ample research efforts before the interview process. The second was crucial in our attempt to expand the knowledge base beyond the available literature. Therefore, most of the questions in our interviews were open-ended, allowing the interviewee to freely express their practical knowledge.

Furthermore, compared to other strategies, the conventional approach was a better fit for our research topic. When considering the direct content analysis strategy, it was clear that in a research topic such as ours, which was not extensively discussed empirically and lacked publications, the strategy would not be effective. Similarly, the summative strategy required a larger dataset, encompassing both collected data and literature material, neither of which was sufficiently available.

4.9 Coding Scheme

Once our content analysis strategy was set, we initiated developing our coding scheme, which did not yet formally exist because of the lack of similar publications on the subject. Our first step in this task was to transcribe the interviews' audio recordings using a dedicated GDPR-compliant software. Next, each researcher went through each transcription, identifying key statements, condensing their meaning, and stipulating its appropriate code and category individually.

Later on, we combined our work and discussed potential improvements. The described approach was important to overcome one of conventional content analysis' main challenges: the misinterpretation of data. Among the multiple options highlighted by the authors to overcome said challenge, peer reviews are one among them, increasing the coding's results trustworthiness [28]. Therefore, each researcher performed three readings of every transcription individually, comparing results after each step. The first was intended to paint a big picture, an important step in interpreting the interviewee's opinions. In the second, keywords were highlighted, and recurring themes were identified. In the third, notes were taken, and keywords were finally grouped into categories. The result of this process is depicted in the following table.

Quote	Condensed Meaning	Code	Category	Sub-Category
What actually changed is, let us see, the question of data storage, because before, it is important for companies that they store their data, you know, or maybe special or personal data that is not allowed anymore, so they need to store that in China now	Data storage requirements changed, personal data must be stored in China	Localized Data Servers	Compliance Action	Technology

It must also be said that, given the small sample size, it was important to use all relevant contributions. Therefore, the team conducted a 1:n statement mapping so that a single contribution could be sorted into multiple categories. For instance: "*There is a reference to certain industries. (...) if you are working in these industries, you have to be careful. In those industries, you may not transfer data abroad unless you have clearance security, the so-called security assessment by the cyberspace authority of China*," (our CMP03 interviewee - 5th of April 2024), was coded as both: "Industry-Specific Requirements" and "Clearance Requirement." The result of this process was the creation of nine categories with three to five subcategories each, 302 entries, and 187 different codes. The following depicts said categories.

1. Compliance Action
    a) Administration
    b) Strategy
    c) Technology
2. Compliance Challenge
    a) Administration
    b) Strategy
    c) Technology
3. Compliance Advantage
    a) Individual
    b) Company
    c) Government
4. Compliance Disadvantage
    a) Legal
    b) Costs
    c) Operational
5. Compliance Control
    a) Enforcement
    b) Goal
    c) Background
    d) Regulation Changes
    e) Industry Restrictions
6. Small-Medium-Enterprises (SMEs)
7. Data Protection Officer
8. GDPR Comparison
9. Impression
    a) Positive
    b) Neutral
    c) Negative

To equip the reader with a full grasp of the meaning behind each category, the following paragraphs will be dedicated to explaining said scheme. Further details on sub-categories will be provided in the subsection, where the results are exposed for each sub-category individually.

Compliance Action refers to changes caused by the regulations with regard to how companies operate, while Compliance Challenges focuses on the challenges faced by companies when attempting to become compliant. After carefully considering the collected data, the research team identified Administration, Strategy, and Technology as appropriate sub-categories for both categories, as they had similar topics.

Next, Compliance Advantage aims to describe advantages brought by the laws, subdividing them into the benefited party: Individual, Company, and (Chinese) Government. Now, utilizing the same sub-categories for the pairing category, Compliance Disadvantage, proved to be nonsensical since there was no sufficient range or volume of contributions by interviewees related to the governmental or individual level. Therefore, the category's subsections were evaluated into company-related subsections, namely Legal, Costs, and Operational.

The fifth category, Compliance Control, aims to encompass all regulation-relevant information from the authorities' perspective, including Enforcement, Goals, Background, Regulation Changes, and Industry Restrictions details. Of course, it must be said that no government offi-

cials or representatives were sourced in this research. Our results are merely the assumptions and impressions of industry members, not official governmental statements.

The following category, Small-Medium-Enterprises (SMEs), touches upon many previously mentioned categories, challenges, disadvantages, and actions, however with a focus on SMEs. They were a major point of attention from the interviewees' side, convincing the research team to have a separate category to address specific changes to the largest company size group in China, "contributing to over 60% of total GDP, 50% of tax income, 79% of job creation and 68% of exports" [29] GDPR Comparison refers to any reference or parallel to the GDPR, a regulation with which German companies have been working closely since it came into effect on May 25th, 2018 [30].

Lastly, the Impression category captures the different perceptions of the regulations, sorting them into positive, neutral, or negative. Now that the coding categories have been briefly clarified, the next section will present our interview results.

5 Results

As a result of the coding process, we now had quantitative data at our disposal. In this section, we will present the collected data and, in turn, prepare our foundation for the analysis section.

5.1 Sourcing Results

Before proceeding with the interview results, we would like to describe our sourcing results. The convenience sampling method has been shown to have some disadvantages, mainly the low response rate of 6.2% after reaching out to approximately 717 people or companies, sending 622 emails in total. We attempted to contact 43 professionals via a networking platform, 44 companies via website forms, and six individuals from our personal network. In total, 299 individual companies were contacted. We received five questionnaire responses, 20 interview confirmations, 18 rejections, and no response from 653 contacts. The table below depicts these results:

Sourcing Result	**Count**	**%**
Confirmed	20	2.79%
Questionnaire	5	0.70%
Denied	18	2.51%
Contact Failed	21	2.93%
No Reply	653	91.07%
Total	717	100%

Table 5.1: Sourcing Results

5.2 Interview Results

We will now depict our research results following our interview's underlying structure. This structure has proven to help guide interviewees through this difficult topic, motivating our research team to share the results accordingly. The following table displays the results of the coding process.

To provide a clearer understanding of our sample group, identify potential biases, and understand the response's context, the research team categorized the interviewed companies

Category	Sub-category	Code Count
Compliance Control	Enforcement	26
	Goal	16
	Background	8
	Regulation Changes	5
	Industry Restrictions	4
	Compliance Control Total	59
Compliance Action	Technology	18
	Strategy	15
	Administration	15
	Compliance Action Total	48
Compliance Challenge	Administration	26
	Technology	11
	Strategy	9
	Compliance Challenge Total	46
Compliance Advantage	Company	22
	Individual	14
	Government	7
	Compliance Advantage Total	43
Compliance Disadvantage	Costs	24
	Operational	12
	Legal	5
	Compliance Disadvantage Total	41
Impression	Negative	21
	Positive	6
	Neutral	4
	Impression Total	31
	GDPR Comparison Total	13
	SMEs Total	10
Data Protection Officer	Yes	6
	No	4
	Data Protection Officer Total	10
	Total	**301**

Table 5.2: Category and Sub-category Code Counts

before analyzing the interview results. Furthermore, each company was identified with a code word in CMP<ID> format to ensure anonymity. All mentioned quotes will be referenced with said code and the interview's date as in CMPX, (1st of January 2024).

The following graph shows the size of the companies interviewed. To define the categories, we utilized the definitions provided by the Organisation for Economic Co-operation and

Development (OECD) of "small enterprises (10 to 49 employees), medium-sized enterprises (50 to 249 employees) and large enterprises (250 or more people)" [31]. This visualization clearly shows the dominance of large enterprises in our sample. This sample feature further reinforced our belief in our results' validity, as larger companies were mostly aware of and acting upon the regulations, as shown by the following results.

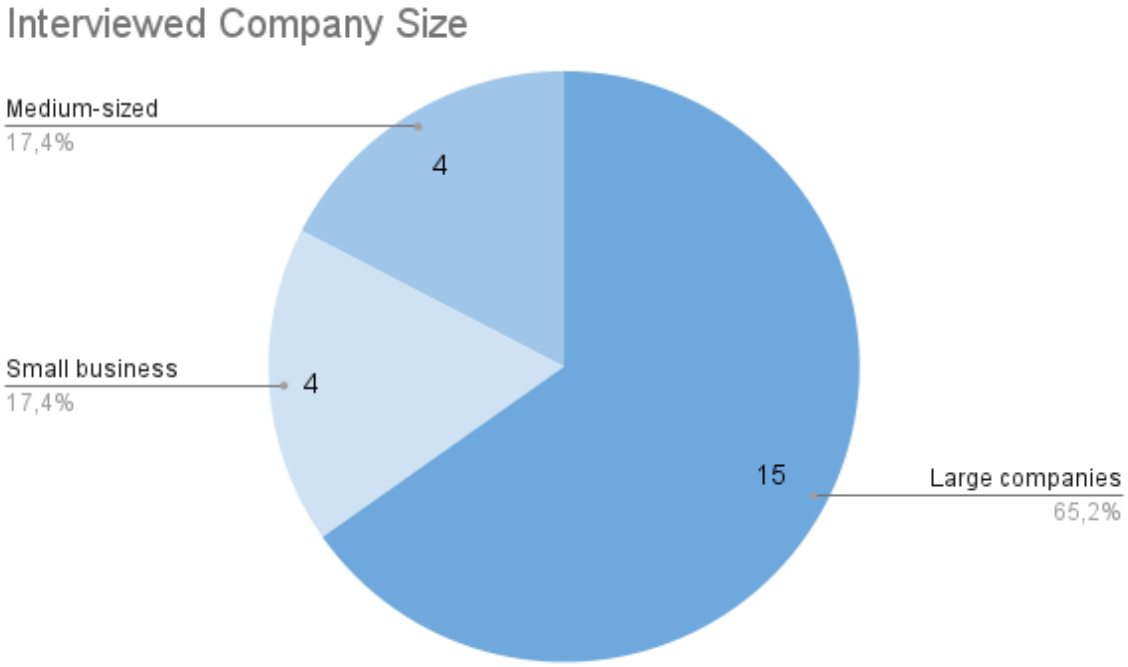

Figure 5.1: Interviewed Company Size

The following graph illustrates the distribution of industries in our sample. Consulting firms occupied a significant part of interviews and contributed to enriching our knowledge on the topic, as multiple experiences with clients in different industries were shared. The combined category of engineering and manufacturing companies comprised the largest portion due to the large amount of areas this categorization covered. Law firms were the third largest interviewed group. They were extremely helpful in contributing factual, theoretical, and practical knowledge, whilst engineering and manufacturing firms aided our comprehension of how the regulations were perceived outside legal contexts. The diversity of interviewed companies gave us confidence in our data's reliability.

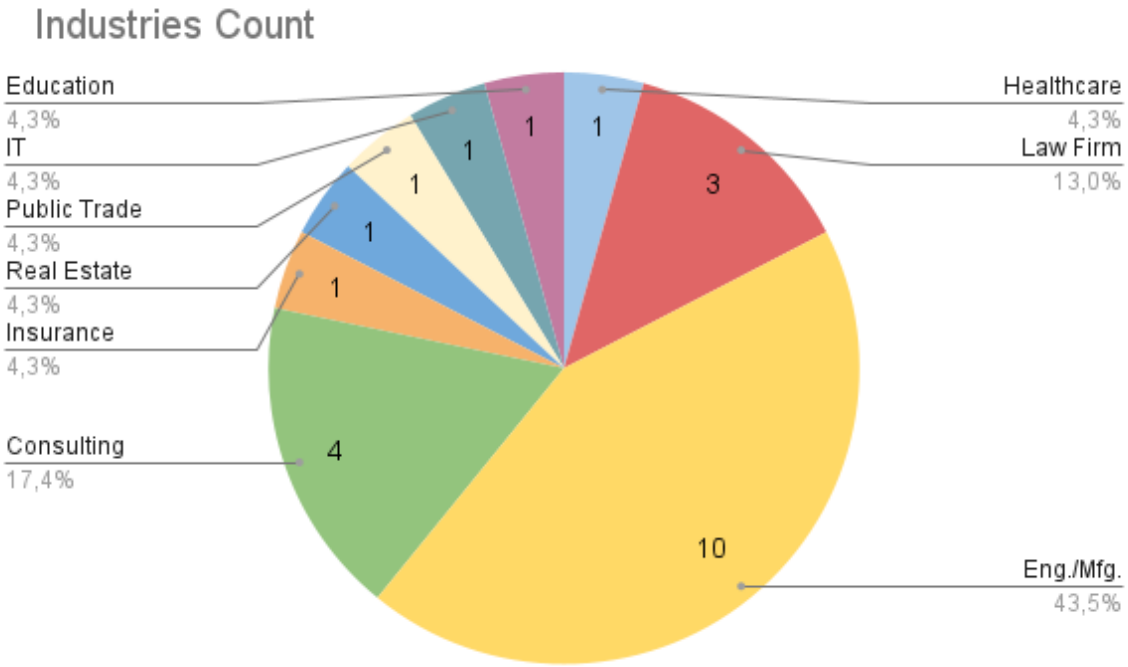

Figure 5.2: Industries

5.2.1 Operation Status in China

The first topic in our interview process was the operation status of the company represented by the interviewee. In its first iteration, the question was too broadly defined. To minimize the need for research interpretation, we restructured the question, defining four clear categories for interviewees' self-categorization: Advanced - operating flawlessly and at full speed, Intermediate - well established with some minor issues, Introductory - adapting, with some issues, and Precursive - initiating and taking the first steps to enter the market.

Moreover, even after restructuring, interviewees still had difficulties understanding the categorizing purpose of this question and often elaborated thoroughly on their companies' operations in the Chinese market. The passionate and thorough descriptions provided by multiple interviewees regularly challenged our intention of controlling the interview's total time to stay within our original stipulation of thirty minutes. After all, as various contributors had busy schedules, spending precious time on the first question could risk a premature interview conclusion, leaving later questions unanswered.

The interviewers had to learn to politely excuse thorough interviewees and guide them to the following questions. Although not planned by the question's scope, descriptions of company operations and journey, proved to be valuable in deepening our background knowledge of the interviewee and company beyond our sourcing efforts, with some even sharing research-

relevant insights, as seen in the following example by our interviewee from CMP01, *"Our team consists of lawyers like myself, we have sinologists and also technicians. And we help the companies on every aspect, including technical and cultural aspects, because as I mentioned earlier via email, it is not just the written law that sets the tone, but more so the bureaucratic enforcement,"* (19th of March 2024).

However, the question's original intent provided valuable insights into our interviewing sample. It was clear that most respondents self-categorized as fully integrated in the Chinese market, as only one interviewee believed their company was in an introductory phase and two interviewees described an intermediate integration level.

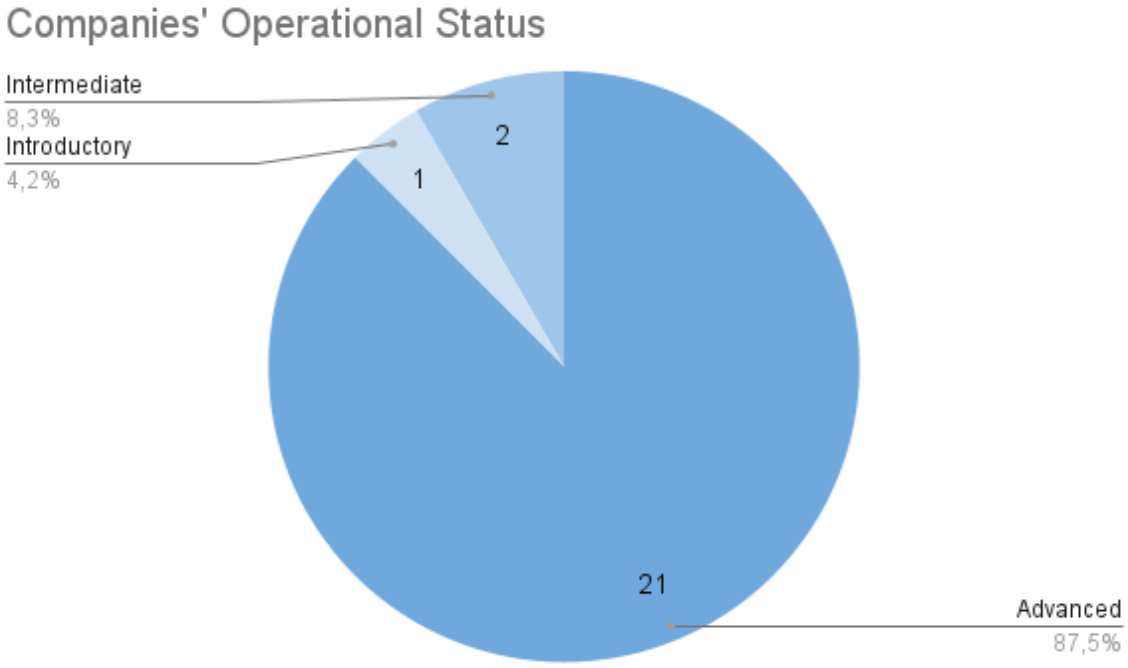

Figure 5.3: Companies' Operational Status

5.2.2 Familiarity with the Regulations

Moreover, familiarity with the regulations was also a topic that required investigating. Understanding how knowledgeable the interviewees were was important for interpreting results accordingly. Additionally, a high comprehension of the regulations could indicate compliance advances in the market.

An important remark to be noted here is that, despite our best sourcing efforts, most interviewees were directly or closely working with the topic, as these professionals were more willing to contribute to our research. This could potentially lead one to the false impression

that most companies are well-informed and compliant with the regulations. However, our sample size was neither large nor sufficiently diverse enough to be considered representative of the population, a common issue with our selected sampling method [32]. To generalize our findings without said remark would be a mistake. For more information on the sourcing process, please check the sourcing section 4.6.

The results here were mostly harmonious. Given that out of twenty interviewees, only five were not directly working with some data protection regulations or did so in the past, this result was expected. After being asked about familiarity with the regulations, most interviewees elaborated on their experience in the industry, mentioned several requirements, and some even touched upon the GDPR for comparison. This showed the interviewee's willingness to share information but also touched upon questions we had planned for later stages of the interview. Having recently engaged extensively with literature on the topic, most of the provided information was already familiar to us. However, in many cases, interviewees mentioned aspects of the regulations that did not surface in our research material. One example from our interviewee from CMP10 was, *"I would start with the oldest one, with the cybersecurity law. It is not very relevant to us since we are not in a critical infrastructure. So we are a B2B business and not for critical industries,"* (10th of May 2024).

Next to obtaining unscripted contributions, we also intended to assess each interviewee's knowledge of the topic. The reassurance of knowledge in the domain was important to validate given opinions. After all, a false expert could pollute our findings with inaccurate information. Although the interviews did not require the interviewees to be experts, having a greater focus on practical experience, unchecked or inaccurate data from a self-proclaimed expert could harm our results. However, we did not identify any such occurrences (whether intentional or not). Experts responded accurately, whilst non-expert interviewees were honest from the start, stating clearly that their knowledge was limited or were interested in learning more about the regulations: *"I have heard about them, but I never had anything to do with them [the regulations] in my working life, so I know what it is. I have heard about that, I have read a little bit about that, but I never worked with that, with this information."* - our CMP02 interviewee (25th of March 2024). With the previously mentioned remarks in mind, the following graph depicts the general domain of the regulation by our interviewees. Here, it can be seen that a slight majority of our interviewees viewed themselves as highly knowledgeable about the topic, and most of the remaining had an intermediate understanding.

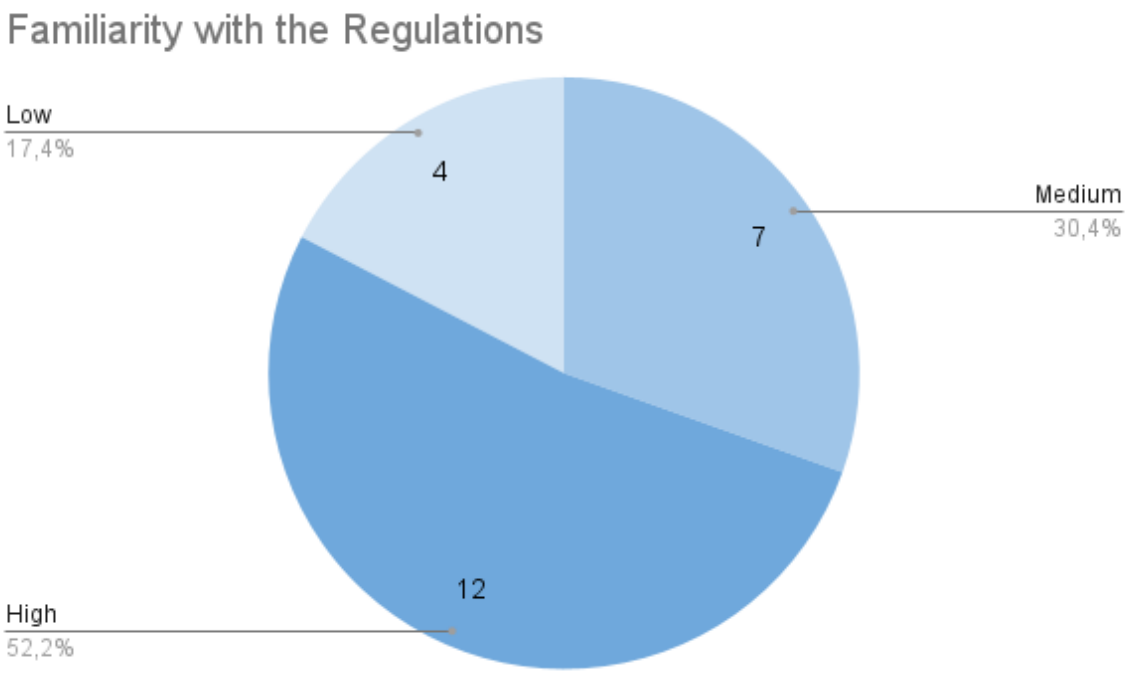

Figure 5.4: Familiarity with the Regulations

5.2.3 Impressions

The next question in our interview process related to the general impressions of interviewees towards the regulations. This inquiry was closely related to our research question, as the regulations' effect on companies and industry members would transpire in their perceptions of the topic. Besides, by interviewing participants from different industries, we could assess if the impressions show some sign of correlation to certain industries. We categorized contributions as positive, negative, neutral, or other (e.g., no position) impressions. This would also allow us to better assess if the provided opinions were biased. We conducted two types of positioning analysis: one at the macro level and one at the micro level.

Macro Level

Considering all contributions by an interviewee, the macro level represented a general categorization of each interviewee's position. After analyzing the interview's results as a whole, weighing the interviewee's underlying tone towards the regulations beyond the number of negative or positive contributions. In other words, this categorization depicted the overlying position of each interviewee. However, contributions proved to be more complex than previously expected. As most contributions were not one-sided and elaborated both positive and negative aspects of the regulations, categorization results skewed towards

the neutral category. The results here show that most interviewed companies are neutral towards the regulations, followed by a few positives, a small group of negatives, and others (interviewees that explicitly mentioned having no clear position). The results reached are depicted in the following figure.

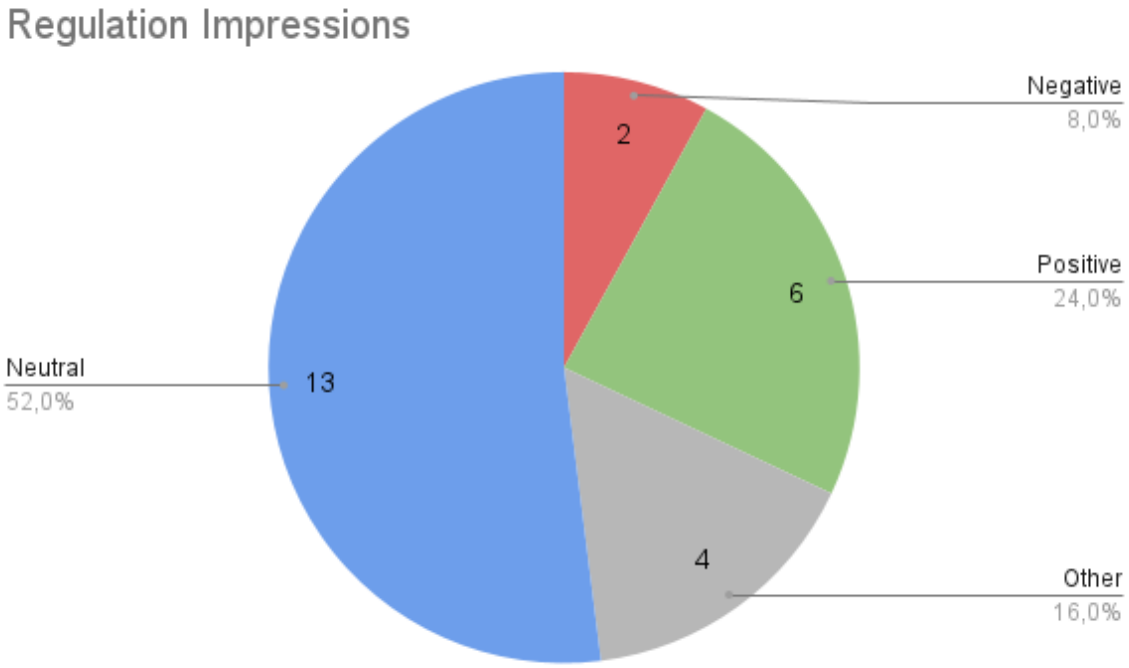

Figure 5.5: Regulation Impressions

Micro Level

The second, the micro level, analyzed each contribution individually. The decision to conduct separate analyses into two levels was crucial because contributions did not always refer to the interviewees themselves but also to clients, acquaintances, or rumors, such as in the case of our interviewee from CM06: "*My company gets hired to view this space and produce these updates because the foreign companies are, or at least were, very worried,*" (24th of May 2024). The results of the process are depicted in the table 5.3.

Impression	Code	Totals
Negative	Anxiety	2
	Challenging	2
	Controlling	1
	Excessive	1
	Overwhelmed	2
	Strict	2
	Sudden	2
	Uncertainty	5
	Vague	4
	Negative Total	21
Neutral	Irrelevance	1
	Necessary	1
	No take	1
	Reasonable	1
	Neutral Total	4
Positive	Justified	1
	Mostly Clear	2
	Positive	2
	Unproblematic	1
	Positive Total	6
	Total	**31**

Table 5.3: Regulation Impression Code Counts

Upon further analysis, it becomes apparent that most codes are negative (more than three-fold the positive or neutral ones), which strongly contrasts the results of the previously mentioned graph. However, this only reinforces the need to separate micro and macro analysis. After mentioning multiple negatively toned statements, multiple interviewees still positioned themselves neutrally, emphasizing that although difficult or overwhelming, the requirements were still necessary and sometimes even positive. For instance, an interviewee mentioned, "*We feel that it [the regulatory efforts in China] makes sense. And it is really not just about putting restrictions on companies, but more so on actually enforcing good data security and data protection practice*"; and "*There is still something we [European data protection regulators] can learn from them [Chinese data protection regulations],*" (CMP01 - 19th of March 2024).

The mention of negative feelings or impressions occupied the majority of results. The lack of clear, official information and definitions proved to be a major source of anxiety for businesses. The vagueness of the regulations and the feeling of uncertainty were mentioned five and four times, respectively, confirming many ideas we gathered from the literature. Our interviewee from CMP04 also touched upon the issue from an individual's perspective: "*And there is a certain reluctance now of auditors going into China just out of fear that they may be reprimanded based on the fact that they collect data, and yeah, and so forth,*" (5th of April 2024).

Interestingly, the result showed a conflicting perception of the regulations. While an interviewee from CMP01 shared that the regulations were getting stricter, the respondent from CMP13, stated that they were becoming more flexible. Respectively, "*We feel that they are getting stricter, by the day, really because China has this national policy regarding, well, national security*" (19th of March 2024). "*So I am thinking right now, especially with the new regulations that the government issued in March of this year, it is pretty more relaxed than before,*" (13th of May 2024).

Said duality in perceptions of the regulations was surprising, and further divergent opinions were shared with each interview. For instance, our interviewee from CMP12 shared that the regulations are clarifying and necessary for the dynamic Chinese market. Our respondent from CMP16, on the other hand, stated that many requirements are unclear, and the regulations have a lot of room for interpretation, respectively: "*If there are no regulations, then you do not know what can happen, if you will get penalized for what, etc. So, we are happy that there are new regulations, new data protection regulations coming in China. And we, we think it is a good thing in general,* (10th of May 2024)", and "*So right now there are a lot of areas also, which are up to interpretation and where there is no corresponding standard or let us say experience. How do authorities interpret certain legal topics there, certain definitions are not yet done,*" (6th of June 2024).

5.2.4 Compliance Actions

Next, questions were asked to delve deeper into the practical changes brought by regulations. In transitioning to this part of the interview, interviewees were informed of the section's importance as a central part of our empirical study. By separating the relatively broad question of "Which changes did the regulations generate in your company?" into three smaller, more specific questions, interviewees provided us with deeper responses. One drawback of this approach was that changes outside our three investigated categories, such as those in R&D, marketing, or sales, could be excluded. For this reason, achieving a balance between clarity and flexibility in the selected categories was key. After multiple iterations and discussions, the research team reached the following pillars: strategic, administrative, and technological changes.

Strategic

The first category to be investigated was strategy. Prior research on the topic, especially publications from consulting firms, highlighted the importance of adapting strategy to regulation requirements as needed [20]. Some remarks that were expected by the research team were restructuring or improving communication with local authorities, data collection, or business model reevaluation. The following graph illustrates the number of mentions for each code in the "Compliance Action" category under the "Strategic Changes" sub-category:

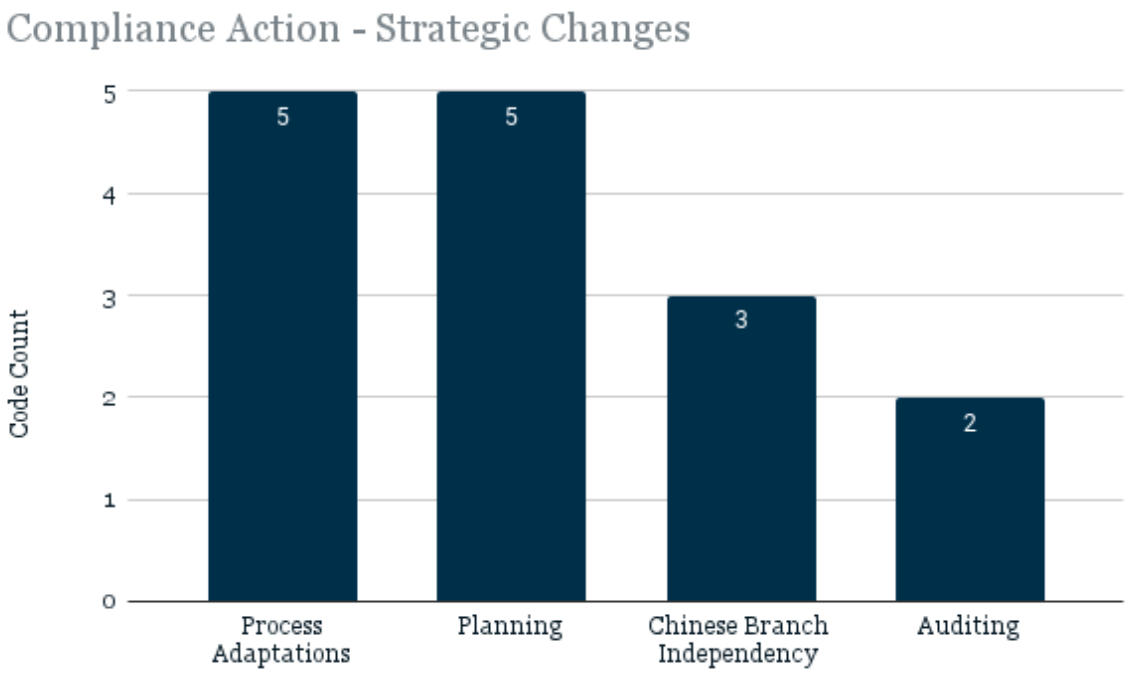

Figure 5.6: Compliance Action - Strategic Changes

One of the most mentioned strategic adaptations was process adaptation, which encompasses all process-related changes. Our interviewee from CMP14 mentioned that contracts had to be reworked similarly to when the GDPR came into effect in Germany. They also shared that accommodating their processes was especially crucial when involving transnational communications or client data: *"this was the same, with the PIPL and the GDPR from Germany. So we are always a little bit ahead, especially in compliance issues. Anyway, we had to accommodate and modify a little bit basically when it was about storing data, when it was about transnational communications (...). For this purpose, we have modified and renewed all our contracts. They were adjusted to the new regulations,"* (1st of June 2024). Our CMP18 interviewee (4th of June 2024) went deeper into said adaptations, mentioning that third-party due diligence process reports containing public officials' names and data had to be reworked, as this type of data would categorize the data as national security. Lastly, our CMP17 interviewee (24th of May 2024) talked about a global movement to create a data protection management system in their company. More details on the system were not provided.

In addition, the increase in independence of Chinese company branches from headquarters was also mentioned. By strategically isolating local HR systems from certain data transfers, companies were able to avoid being classified under certain regulatory categories, as described by a contributor: "*So basically it was more about an operational implementation. We cut off certain data transfers from our local HR system into the global HR platform,*" (CMP1- - 10th of May 2024).

Another interviewee (CMP18 - 4th of June 2024) expanded on the topic, mentioning that some HR interfaces were changed in the Chinese version of the company's global operational tool. Personal data such as names or email addresses, normally displayed in the tool's global version, were removed, granting the tool a lower data sensitivity tier and fulfilling some requirements.

Furthermore, given the additional workload and standards created by the regulations, Chinese divisions had increased responsibilities and roles. Increasing the division's independence to better adapt to the requirements seemed to be a common strategy within multinational companies in the Chinese market. One of said responsibilities is risk assessment, which is closely related to auditing; another mentioned strategy action by multiple interviewees: "*You check and double-check your contracts, you check your servers, you check your way how to handle data inside your company and maybe with external partners,*" - our CMP14 interviewee (1 st of June 2024). Auditing is mentioned as a powerful tool to identify non-compliant processes and assess if a given measure effectively contributes to risk mitigation. "*Whether these measures are really adding to the project to mitigate the risks is a really difficult question. So maybe auditing is a very necessary and a very useful thing for people to really implement privacy compliance,*" - our CMP17 interviewee (24th of May 2024).

Administrative

The next category to be analyzed in our questions was administration. This pillar aimed to encompass all business-related operations, such as HR, negotiations, communication, legal matters, and finance. The following graph illustrates the number of mentions for each code in the "Compliance Action" category under the "Administrative Changes" sub-category:

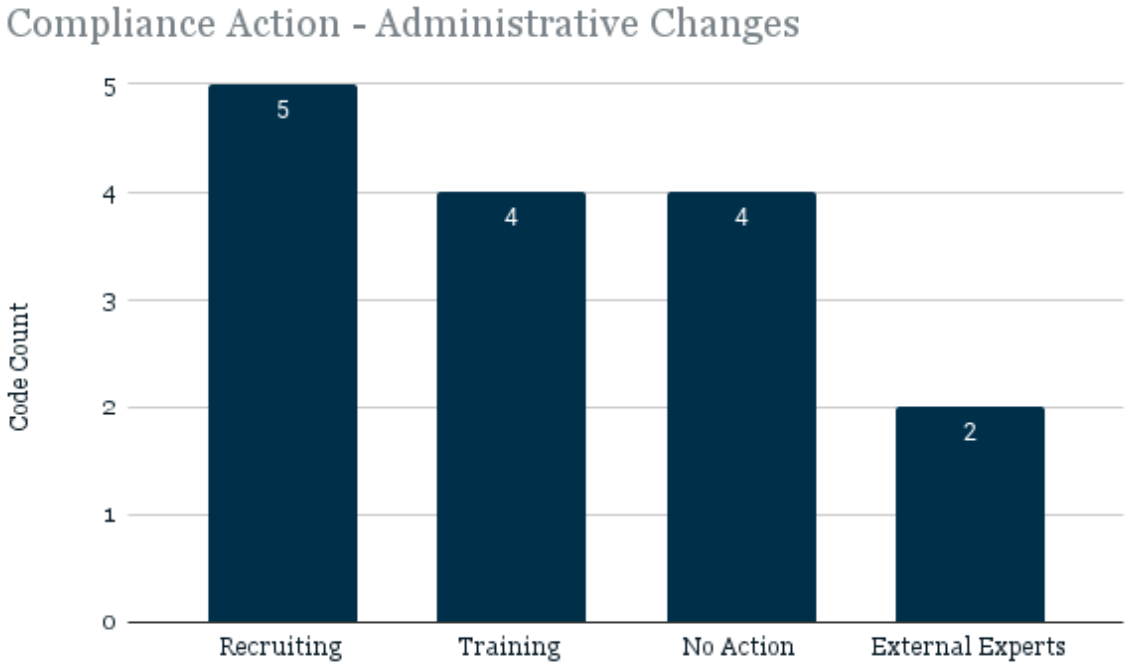

Figure 5.7: Compliance Action - Administrative Changes

Training occupied 26,7% of key administrative changes mentioned by the regulations. How said training was conducted varied. Some interviewees (CMP16, CMP14) mentioned workshops or seminars where company members (or client companies) were instructed on the regulation's requirements. Others mentioned more formal approaches to training, offering legal teams the opportunity to deepen their knowledge of the laws (CMP01, CMP15, CMP10). A clear focus was given to legal teams, which, given the complex legal intricacies, play an important role in advising management and further departments and assessing compliance status: "*Well, our legal department naturally is heavily involved with all these kinds of regulations, and then they advise other sections of our company on basically what to do, what is allowed, what is not to be done, and so on and so forth,*" (19th of May 2024).

Hence, the importance of HR and recruiting is another greatly mentioned topic in the interview process. When teams could not keep up with the increasing workload and complexity, enterprises opted to hire additional legal experts: *"We also hired a specialized lawyer who now is responsible for the topic,"* (our CMP18 interviewee - 4th of June 2024). The role of this professional is further described in this contribution: "*We hired an external lawyer who additionally supported us in the analysis of all of these laws and where we stand and had a local implementation project where we tried to make sure to get all of the things done, like the impact assessment, like the getting, the consent and so on,*" (our CMP10 interviewee - 10th of May 2024).

Our last observation from the collected data was that three interviewees (CMP02, CMP05,

CMP10) mentioned having no or little additional administrative actions after the regulations were enacted: "*[speaking about PIPL] To be honest, to our daily business, there is no effect generally because our business scoreboard is not so huge*" (CMP05 - 15th of May 2024).

Technological

The final pillar examined in this section was technology. While data protection regulations are typically linked to technical requirements, the Chinese law triad under consideration in this research appeared to impose even stricter constraints than comparable regulations worldwide. The following graph illustrates the number of mentions for each code in the "Compliance Action" category under the "Technological Changes" sub-category. The 3 codes identified in this section were: Data Organization, Data Localization, and Cross Border Transfer.

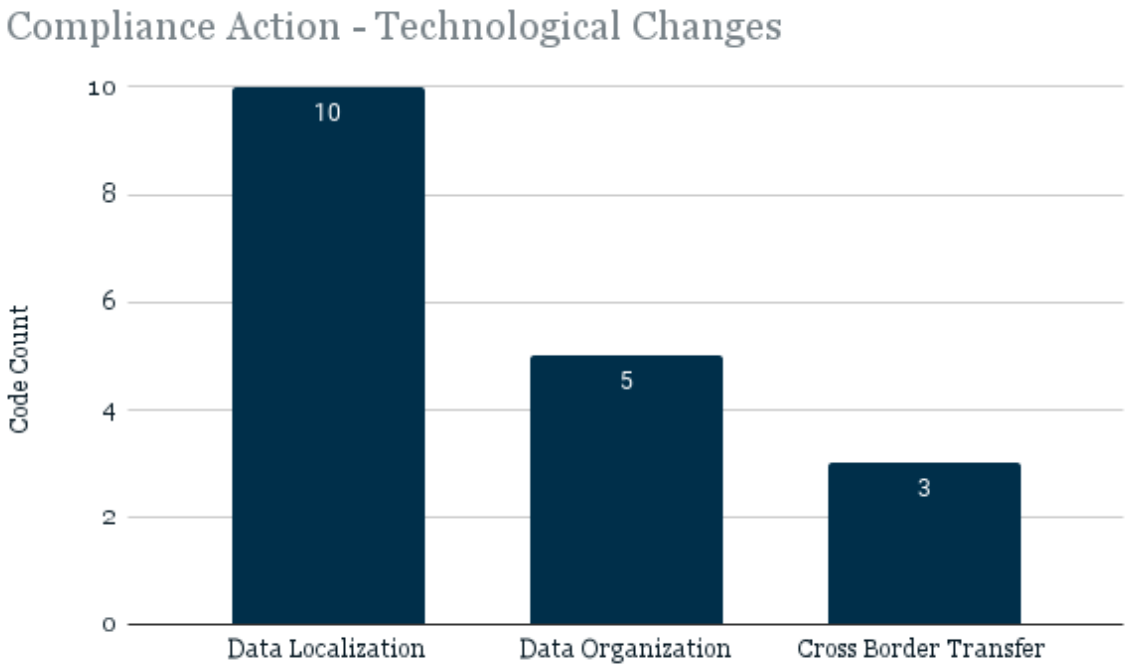

Figure 5.8: Compliance Action - Technological Changes

A first glimpse at the results is sufficient to identify the predominance of Data Localization mentions. This parallels with large quantities, to which the requirement is explored in multiple publications. It is no surprise that interviewees were aware of said specifications. However, empirically, the approach with which companies are fulfilling these conditions is diverse. While an interviewee (CMP10 - 10th of May 2024) mentioned operating with a centralized IT infrastructure in China, 2 others (CMP01, CMP15) stated the attempt to diversify their databases, moving data centers outside of Chinese territory. Furthermore, our CMP03

interviewee commented: "*a lot of people (that they) bring the whole IT infrastructure into China and keep it within China and avoid sharing the data IT infrastructure with abroad,*" - (5th of April 2024). Some interviewees mentioned the need to build or purchase local data infrastructure from the ground up, as with Apple in 2018 [33]. Furthermore, another contributor (CMP10 - 10th of May 2024) elaborated on a centralized infrastructure, this time in Germany, keeping only the strictly required data in China. Some companies (CMP01 - 16th of March 2024), in an attempt to avoid the regulations, moved their entire IT infrastructure to Europe, Australia, the United States, or other jurisdictions in Asia. However, certain industries require low latency, so server localization might become an issue, as noted by our CMP01 interviewee: "*depending on what kind of industry, for example, internet of things, industry 4.0, they need better frequency, lower FPS, so they tend to go to Singapore or Hong Kong, but for example electronics or just yeah, dealership locations in China, they do not need this high frequency, so they go back to Hong Kong,*" - (19th of March 2024).

The second code in this section, "Data Organization," relates to all actions required from companies in regard to data mapping, categorization, analysis, and classification. An interesting contribution from a large consulting company member enlightened us with the advice given to clients on this matter, namely the importance of understanding what kind of data is being collected: "*This [data organization or classification] is one of the areas where we advise our clients, and then we do that very actively, so normally what we do is, to give you a brief overview of what we do in that regard, normally it is the first step for our clients, to understand what kind of data they collect. So, whether this data is relevant in China, whether it is important data or whether it is personal data, personal information,*" - our CMP03 interviewee (5th of April 2024).

As a company that provides health studies services, an interviewed enterprise had the need to export large quantities of personally identifiable data from Chinese individuals abroad. A workaround found was anonymization: *You just remove the names of the patients and use an ID number or something else. Just erase whatever personal information is out there, and then just get the factual data that you actually need,*" - our CMP11 interviewee (10th of May 2024).

Lastly, Cross Border Transfer was the third code identified. Although closely related to Data Localization, some specific mentions of the topic motivated the creation of a separate code. Its importance and complexity were heavily present in the research material. However, our CMP13 interviewee shared that said complexity can be exaggerated and is mostly dependent on data volume: "*it [cross border data transfer] is not as complicated as a lot of people saw. Only for very big companies. If you are, let us say, you have more than 100, 000 users, of course, that is another thing, but for normal companies, especially SMEs, large to medium-sized companies, I think it is not a big topic at all,*" - (13th of May 2024).

Furthermore, it appeared that the GDPR and the PIPL were sufficiently similar, allowing the expertise from the former to partially transfer to the latter, as commented by an interviewed lawyer: "*But when it comes to the cross border data transfer, thanks to the knowledge that I obtained through GDPR before, I was able to do the data classification and then do all the data mapping,*" - our CMP11 interviewee (10th of May 2024).

5.2.5 Advantages

Analyzing compliance advantages and disadvantages has provided insights into how the various entities currently perceive and have benefited from the new compliance standards. This first section dives into the subcategories of compliance advantages, specifically focusing on the company, country, and individual aspects.

Company

Compliance advantages are complex and multifaceted, impacting operational efficiency, legal risk management, customer trust, and the company's competitive position. For example, our interviewee from CMP14 noted: "*this might also be a competitive advantage for most German companies because usually the German companies have pretty high compliance standards anyway which they apply, and they are coming from the headquarters, and usually they do not search for ways around or gray areas that they could exploit in China*," (1st of June 2024). A culture of high compliance standards should not be underestimated as it could attract more business opportunities.

In certain cases, enforcing compliance regulations has also helped filter out unnecessary information. Specifically regarding the removal of private information, our interviewee from CMP10 stated: "*It also helps a little bit, in my opinion, to reduce unnecessary information. So there have sometimes been slides and, for example, management reviews with names on them, which was absolutely not necessary. You can also do that online*," (10th of May 2024). Hence, removing unnecessary information could increase efficiency and internal security.

Many companies have already acquired or built up a database of client contact information over the years before these new regulations were implemented. The need to confirm or reconfirm a client's willingness to use their data bears the risk of losing a large portion of that data. As our interviewee from CMP16 states: "*If you have a, let us say an old collection of this data. And then, you want to make it clean, and you ask everyone, please confirm back and sort of double click that you agreed to receive our information, then you will lose, I guess, 90 percent of the data*," (6th of May 2024). The interviewee, however, also points out that this can be advantageous: "*But in fact, if you look at it, the question is. Also, it is not only a disadvantage because in this 90 percent that you lose, if they do not read your emails, why do you want to have them on board? So it is also a chance to clean it up*," (6th of May 2024). Weeding out 90% of your database might look horrendous on paper, however, the 10% of clients that are left behind are the ones that actually care and are your primary targets.

Furthermore, these new regulations assure clients that the company is reliable when it comes to handling their data, as they are forced to implement certain security practices. As our respondent from CMP03 shared: "*We see more awareness in that regard, and we also see a lot of more responsiveness, and we also have a lot of inquiries with regard to a data protection officer, if we can take that over, if we can support them with the implementation of certain structures and systems. So there is definitely more awareness*," (5th of April 2024). Adhering to compliance standards

consequently also reduces the risk of data leaks. As our respondent from CMP12 stated: "*the regulation sets certain standards on protection of personal data, also cybersecurity you know, data is a very valuable thing in these days. So first of all, if you get the compliance, achieve the compliance with, with local laws you have less risks that there will be a data leakage, for example, which can affect your business,*" (13th of May 2024). Data leakage would massively affect a business due to the negative impact it would have on a business's reputation.

Another advantage to adhering to laws, is avoiding potential legal penalties. As our interviewee from CMP16 puts it: "*I think short term [advantage] is you can protect your company also against any kind of liabilities which might come up in that context. There is always the potential of if you do not follow or if you do not comply that you get some, you know, trouble, illegal way, which could cost actual money,*" (6th of June 2024). These results show that adherence to compliance standards can offer significant benefits. High compliance standards enhance efficiency and reputation and are potentially a competitive edge for companies.

Government

This section will focus on the advantages of compliance from a government perspective. For optimal results, governments have to strike a compromise between having control and fostering enabling innovation. As our respondent from CMP11 notes, "*In a sense, the [Chinese] government is really trying to understand how to best balance between the needs of the government and the needs of the companies,*" (10th of May 2024). The regulations give governments more control over the data within their jurisdiction, as our participant from CMP09 pointed out, "*(...) the Chinese government thus also has more control over what happens with their citizens' data,*" (19th of May 2024). This control helps maintain and ensure national security: "*Of course, there are going to be advantages for the Chinese authorities since with more control on the data, I think they could enforce national security,*" (our CMP08 interviewee - 20th of April 2024).

Another advantage is that compliance regulations enhance a government's ability to intervene in corporate data practices. Our interviewee from CMP01 observed, "*The Chinese state now can audit the companies, the internal IT structure, also the data processing,*" (19th of March 2024). As our interviewee from CMP17 noted, "*Each kind of law, like for export control, maybe also for anti-competition, unfair competition, or something like that (...) could provide more legal certainties for the country and have a better system,*" (14th of May 2024). These laws then, in turn, enable the government to enforce their decisions, as our interviewee from CMP12 shared in this example, "*[a given company] was fined 1.2 billion dollars,*" (10th of May 2024).

The Chinese government can furthermore use compliance regulations to enhance national cybersecurity. This is necessary, as our participant from CMP06 points out, "*an advantage is, if your business operations are more and more dependent on data and what happens in cyberspace, there is of course also a need to feel safe and to be protected from malicious actors, like hackers or the competition doing something with your data,*" (24th of May 2024).

Furthermore, data is increasingly viewed as a valuable national asset. It naturally makes

sense for a government to attempt to retain control over such a valuable resource. As our respondent from CMP12 notes, "*For a Chinese government as for any other government, data is very valuable. It is a new gold, right? So they are trying to keep the data within China,*" (13th of May 2024). By regulating data export and handling, governments can retain control over this valuable resource, using it to leverage economic and strategic advantages.

From the Chinese government's perspective, implementing these new data protection laws provides significant benefits regarding control, security, and political leverage. Certainly, these regulations enhance China's control over its cyberspace.

Individual

Data protection regulations also offer significant advantages for individuals, impacting employees, consumers, and citizens. The following section will examine those advantages.

One critical advantage is that new regulations can help bring awareness to certain topics. As our interviewee from CMP03 states, *"raising that awareness and the protection level, I think that is an advantage because it protects the individual,"* (5th of April 2024). The regulations will make companies more hesitant about deliberately maliciously using private data. As our interviewee from CMP13 puts it, *"I think it is [the regulations] going in the right direction because I think nobody wants the companies to play too much with the data, right?"* (13th of May 2024). This stance is shared by many of our interviewees, including our interviewee from CMP04, *"to protect the citizens' data, like, and also protect it from unlawful export, transport, transfer, and make it very clear what rules have to be followed when intending on doing so,"* (10th of April 2024). Our interviewee from CMP03 echoes this stance: *"data is something which has to be protected, in particular when it comes to personal information, that you may not float around personal information,"* (5th of April 2024).

Another advantage is that it makes it harder for companies to sell their users' data. As stated by our interviewee from CMP17, *"I get some like a trash email or get some spam or get some random call from some companies, whether they are stealing my data or something like that,"* (24th of May 2024). New data protection regulations can help ensure that an individual's data is kept safe from data breaches and misuse. They also help individuals feel safer and increase company trust.

In summary, for larger companies, the new laws can potentially enhance efficiency, help them improve their reputation, and reduce the risk of a data leak. Compliance standards benefit the government, as they provide the government with more leverage, enabling it to intervene and ensure national security. Individuals also benefit, as an increase in awareness and responsibility towards protecting user's data, helps build trust and security.

5.2.6 Disadvantages

Covering the perceived disadvantages is as equally important as the disadvantages for our research. The following graph depicts our results in this section. In the following subsections, we will analyze each pillar individually.

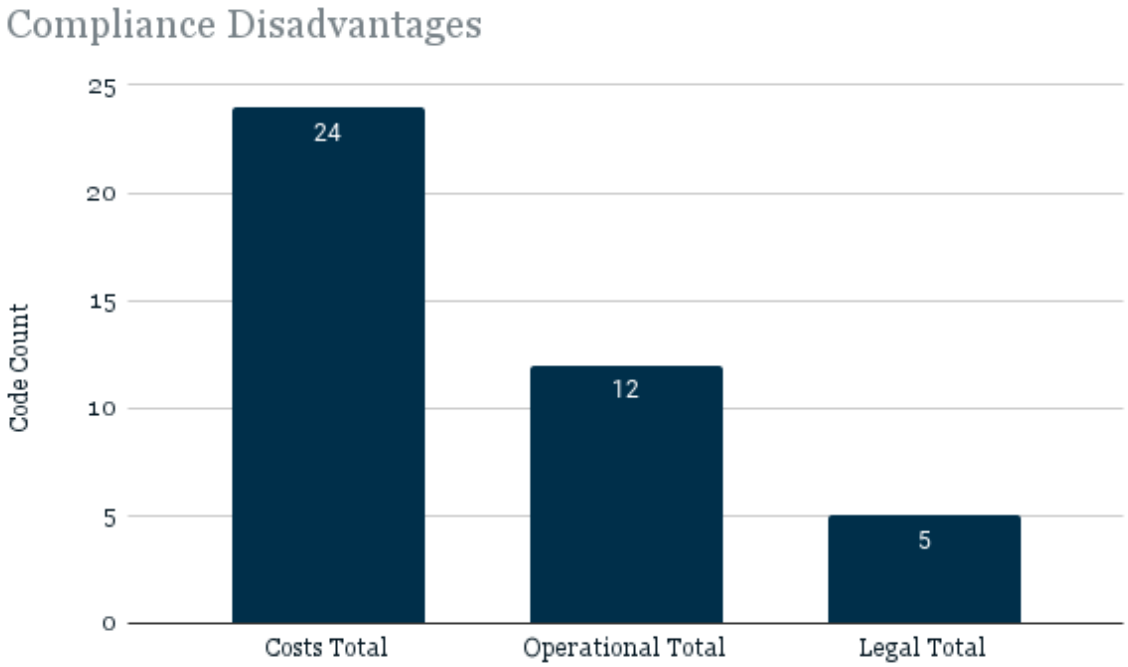

Figure 5.9: Compliance Disadvantages

Legal

Starting with the least mentioned category, any new laws that impact a business can often impose significant legal burdens on a company. These include the need for lawyer consultation fees, an increased risk of legal penalties, and the risk of sensitive information leakage. Legal issues often complicate business operations and divert resources from core business activities. The following section looks deeper at the potential legal disadvantages of the new data protection laws. The coding results for this section led us to five codes: Risks Confidentiality, Challenging Legal Interpretation, Legal Burden, IP Protection, and Fraud.

For larger companies, introducing a new regulation might be just another legal complexity as our interviewee from CMP05 puts it, "*To the big agency, they will consider this as an extra like legal issue to their department*," (15th of May 2024). With each new regulation, legal departments must dedicate ever increasing amounts of resources. Each new regulation also increases legal complexity, making it harder to abide by all rules. Furthermore, as our participant

from CMP04 noted, "*And the more vague or the easier, well, the wider it is to interpret such laws that create more costs to ensure the interpretability is as narrow as possible,*" (10th of April 2024). This vagueness further increases complexity and requires frequent consultations with legal experts to be properly interpreted. As these new data protection laws are evolving and being updated, legal consultations need to be just as frequent and are a constant financial and human resources cost.

Looking a step further, compliance with the new laws will also add certain risks concerning confidential data. Our interviewee from CMP05 pointed out, *"The data processing not only concerns personal information but also non-personal information, which might be business secrets as well,"* (15th of May 2024). Giving the government access to conduct audits naturally bares the risk that these access rights can be exploited. This is further reinforced by our respondent from CMP18, who stated, *"One of our greatest concerns is IP protection,"*, and more specifically, *"appropriation of company assets, or basically fraud*, (4th of May 2024). This is a direct follow-up of the prior disadvantage, as the increased scrutiny and documentation required for compliance can create opportunities for fraudulent activities.

In summary, introducing new laws can significantly burden businesses by increasing legal costs, risks of sensitive information disclosure, and compliance complexities. Larger companies see regulations as additional legal complexity, consuming their resources. Vague laws make the situation more complex, requiring frequent and costly legal consultations. Another legal disadvantage mentioned by interviewees is compliance risks, which include exposure of confidential and non-personal information, such as business secrets, during government audits, as well as heightened concerns over IP protection and potential fraud.

Costs

Companies, especially larger ones, face ever-increasing costs when implementing and abiding by the new laws. These costs come about for many reasons, including the need for additional personnel, training, legal advice, and restructuring. Cost also happen to be the category that most individuals can directly relate with resulting in significantly more coding entries. The subsequent section examines the cost-related disadvantages of the new data protection laws.

The first major cost factor is one that was pointed out by our interviewee from CMP07, *"A great disadvantage, or it is a disadvantage for the company, I would say it is dealing with the whole restructuring,"* (19th May 2024). Due to the new laws, international companies often needed to restructure their operations and individual departments. A major restructuring naturally involves significant financial costs, disruptions to business operations, and a period of adjustment where efficiency will be negatively affected. All of which have negative financial repercussions. Even in cases where no strategic changes were necessary, other operational costs are still prevalent, as our interviewee from CMP10 states it, "*So basically, no strategic changes, but it definitely increases the compliance cost*," (10th of May 2024). Another aspect concerns how companies also face high costs for external administrative audits. This was specifically pointed out by our interviewee from CMP01, "*[talking about compliance cost sources]*

This can be from the external administrative cost, for example, for auditing fees by public bureaus. This can be tens of thousands of euros, for example, or the overall cost you need for the internal budget can go into the millions because you have to set aside your personal expenses," (19th of May 2024). Recurring audits, while advantageous (as explained in the previous section), are extremely costly, according to the interviewee. Additionally, failing an audit can lead to costly penalties and the need for expensive corrective actions.

Compliance also requires budgeting for internal costs, including personnel expenses. Hiring specialized compliance officers, legal experts, and additional administrative staff to manage compliance activities, which can all significantly increase payroll expenses. These roles are essential to ensure compliance protocols are followed, but they add to the overall operational costs. This disadvantage is highlighted by interviewee CMP01, who stated, "*So this [adapting to regulations] means more internal costs. They have to budget this. This can be from the external administrative cost, for example, for auditing fees by public bureaus. This can be tens of thousands of euros, for example, or the overall cost you need for the internal budget can go into the millions because you have to set aside your personal expenses, which also costs and for that as well,"* (19th of May 2024). Another costly expense is regular compliance training. As mentioned by our interviewee from CMP10, "*We have to do regular trainings. We have to develop the training and so on,*" (19th of May 2024). The training itself incurs direct expenses, and the cost associated with time allocated to training instead of usual tasks results in additional financial burdens.

These significant time investments can also be caused by other aspects and often even involve top management. "*A lawyer can only process things when he knows what he should process, so we really spent a lot of internal hours on the topic and if it should be just a ballpark number I would say something between one hundred to two hundred hours. That is often also on director level and above, so really top management resources in the end*" (10th of May 2024), stated by our CMP10 interviewee. As previously mentioned, time spent on compliance actions, especially by senior management and key personnel, can decrease overall productivity. Furthermore, their time is also worth a significant amount due to their high positions and large paychecks. An interviewee stated that larger companies face higher compliance costs: "*for any company that wants to do business in China, (...) the larger the company, naturally, the larger the cost. The larger you are, you will need to head to inform yourself with consulting companies and so on and so forth, and then you have to implement all the necessary changes. And it is just a massive amount of cost. Also, like, the restructuring costs, human resources, IT, and so on and so forth. Just lots and lots of costs, and very expensive*" (our CMP09 interviewee - 19th of May 2024). Larger companies have complex networks involving many aspects, including divisions, subsidiaries, and departments. This drastically increases the difficulty of implementing methods to abide by new laws. Once a company surpasses the cumulative transfer of a hundred thousand individuals' personal data [34], the set governmental requirements increase drastically. Conversely, this means that smaller companies can work under looser requirements.

As mentioned in the prior section, the new regulations bring many costly legal issues. This includes the need for legal counseling and interpretation, as stated by our interviewee from CMP10, "*The cost increase, we had to hire a lawyer,*" (10th of May 2024). These fees are

substantial and increase for larger companies with complex structures. Compliance with the new data protection laws necessitates investments in IT infrastructure and human resources. "*Restructuring costs, human resources, IT, and so on and so forth. Just lots and lots of costs, and very expensive,*" (19th of May 2024) highlighted our interviewee from CMP09.

This subsection showed that implementing new laws brings substantial costs for companies, particularly larger ones, due to the need for more personnel, training, consulting costs, and restructuring. Companies must also budget for hiring compliance officers and legal experts, along with regular compliance training, which impacts productivity and consumes internal resources. Larger companies face higher costs due to their complex structures and the need for significant IT and human resource investments. Regular audits and the potential for failing them add further financial strain, making compliance an expensive and resource-intensive task.

Operational

The final type of company disadvantages we noted were operational. These include factors such as increased complexity, reduced efficiency, and the potential loss of autonomy. The following section takes a closer look at these issues.

The first notable disadvantage was mentioned by our interviewee from CMP03. "*Of course, it [the regulations] makes things more complicated. Companies have more administrative burden. They have to obey more rules,*" (5th of April 2024). The need to adhere to various regulatory requirements adds complexity and negatively affects operational efficiency. Furthermore, the new data protection regulations can potentially limit a company's outreach. As our interviewee from CMP16 puts it, "*You also limit outreach for individuals to reaching out to larger crowds of recipients of their information, which, if you use email or things like that to send out data, to send out information about your products, you will have to adjust,*" (6th of June 2024). These restrictions are naturally devastating for certain companies, especially smaller ones.

Our respondent from CMP10 expressed their fears and pointed out another potential issue, "*My fear would be if we do not have a certain autonomy in that area, we will not get the support that we need when we need it in China again, a very dynamic market. The regulations can change very quickly,*" (10th of May 2024). If companies are too limited in what they can and cannot do, they will lose their ability to adapt to a rapidly changing environment. Compliance measures can, however, also complicate workflows as well as make them less efficient. Our interviewee from CMP16 mentioned, "*It makes working workflows in many ways more complicated,*" (6th of June 2024). The disruption of current workflows results in slower productivity as additional steps must be added to stay compliant. Every additional step in a workflow is a further potential point of failure and employees will also need to learn the new steps.

Compliance can also increase the need for manual data processing. A respondent, our interviewee from CMP11, noted, "*We do research in about 14 different industries, and when DSL came out, we had to make sure that we have 14 different data classifications basically. You could put all*

the data in one Excel spreadsheet, but obviously you are gonna burn your computer. So, you have to do it one by one," (10th of May 2024). This need to manually process large amounts of data is a massive disadvantage. These tasks are not only labor-intensive but also time-intensive. Yet another disadvantage is the resource-intensive task of training local employees to handle tasks that used to be done by international ones. This became necessary for certain companies, as certain tasks needed to be handed over to local workers to ensure that the data did not need to be transferred internationally. This issue was specifically mentioned by our interviewee from CMP15, "*The Chinese colleagues had to be brought up to speed, and that took quite a bit of effort*," (15th of May 2024).

Our interviewee from CMP15 touched upon a further issue in regard to data protection regulations potentially hindering global networks. "*Creating digital borders prevents global networks. It forces Europeans to connect to Chinese networks*," (15th of May 2024). These hindrances then slow progression and reduce overall efficiency in global operations. As previously mentioned in our cost subsection, our interviewee from CMP01 mentioned, "*The Chinese state now is able to audit the companies, the internal IT structure, also the data processing*," (19th of March 2024). Frequent necessary audits are costly and hinder, disrupt, and sometimes even completely halt operations.

One possible result of the new regulations was brought to our attention by our interviewee from CMP10. They noted, "*You would have to go the real harsh way and separate your whole IT infrastructure here, but then all of the synergies are gone, and this is not really a feasible alternative for certain industries at least*," (10th of May 2024). This would result in massive operational delays, harm productivity, and force changes to the current working systems. As our CMP10 interviewee also pointed out, it is also quite unrealistic for certain industries.

One final disadvantage came from our CMP17 interviewee, who explained, "*People can take advantage of the laws in a political sense to limit free market development and gain advantages*," (24th of May of 2024). Exploiting regulations in this manner results in operational issues, leading to suppressed competition and innovation.

As can be seen from the responses we received from industry professionals, the new data protection laws have brought along substantial disadvantages that need to be taken into account and thoroughly analyzed. The main categories discussed were in regard to legal, cost, and operational aspects. Legal complications can directly result in operational difficulties. These both in turn cause significant financial burdens, which then further affects operations.

5.3 The Road to Compliance

Following next, we will delve into everything surrounding the final issues regarding compliance that the companies of our interviewees face in order to meet the multitude of requirements set out by the Chinese government. We decided to split these factors into five categories: challenges faced by the company, the assessment from China, the role of a data

protection officer (DPO), the impact on small and medium-sized enterprises (SMEs), as well as a comparison between the GDPR and the PIPL.

5.3.1 Challenges

When it comes to challenges, they are quite numerous and appear in all sorts of shapes and sizes and thus need to be categorized further. Similar to the changes section, the research team decided to reuse the three pillars: the strategic, the administrative, and the technological challenges. The vast majority of the companies interviewed faced a variety of these issues, especially regarding administration.

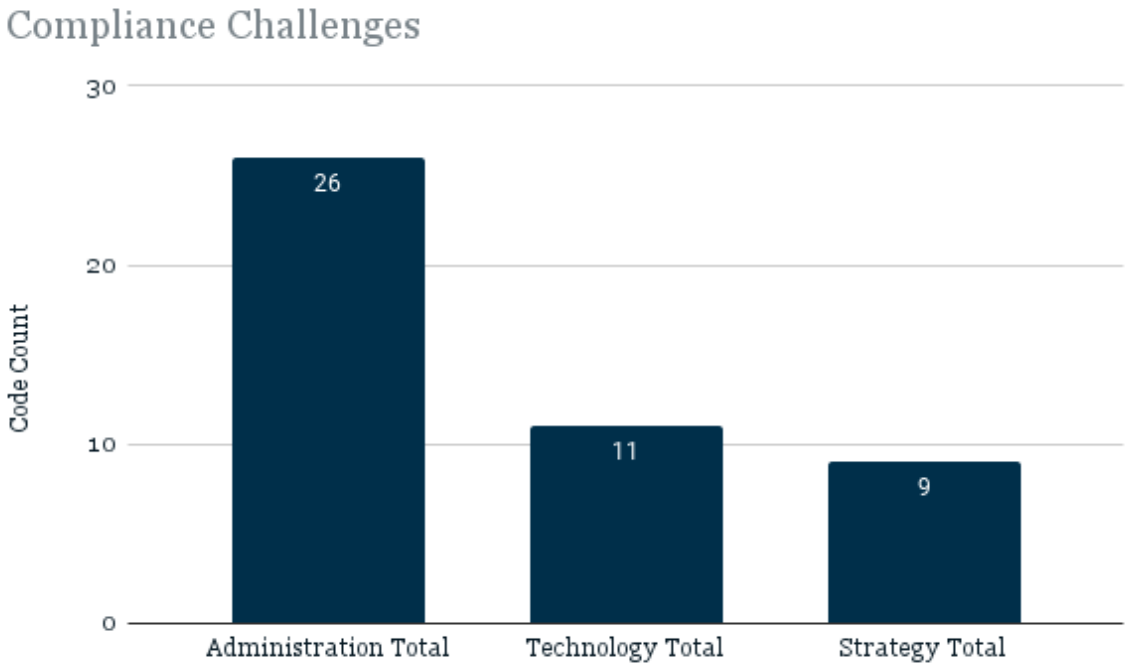

Figure 5.10: Compliance Challenges

Strategic

Due to new data protection regulations, companies have had to face many challenges which forced them to make significant strategic changes.

As stated by our interviewee from CMP18 "*The usage of global platforms, such as HR, make it difficult to comply to so many different regulations across the globe simultaneously,*" (4th of June 2024). In order to stay internationally competitive, companies are forced to comply with a multitude of regulations, all across the globe, simultaneously.

Some issues also arrived due to cultural gaps causing a lack of seriousness when handling the laws from the local Chinese employees who are citizens of China. As, our interviewee from CMP10 states it, "*The biggest issue was that my colleagues, who are all Chinese, did not take it very seriously, which is also understandable because, again, the way how the law works here is a little bit different. And I had to first increase the sense of urgency again, not because I believe that we are suddenly the focus of the authorities,*" (10th of May 2024).

Due to these new regulations and changes, communication aspects for global companies have definitely suffered. They either need to change their current methods or accept the limitations of their current systems. The respondent from CMP14 noted, "*There are a lot of strategic discussions at the moment. As there always are, but in the last few years, especially due to the fact that the communication with the headquarters (...) it was very difficult or even more difficult than before to maintain efficient communication,*" (1st of June 2024).

One of the most worrisome issues about the new regulations, is the fact that nobody can currently be certain what kind of information can and which can not be shared. Even information that can be found on websites that can be accessed by anyone, can be considered as information of national importance to the point that national security may intervene. This exact issue was brought to our attention by the interviewee from CMP11. "*There is a Baidu, like Google. He shared this publicly available research that can be found on Baidu. He copy pasted the link and sent it to the (...) company. The (...) company reviewed it and found it to be fantastic information. National security then comes in and questions why would you share such information? It sounds ridiculous,*" (10th of May 2024). This kind of precedent makes it quite apparent why companies are so anxious about the regulations. Just the fact that the Chinese government can intervene at any point in time is a concerning matter. This kind of concern is, however, also created due to the cultural environment of the EU citizens.

Additionally, our CMP01 interviewee noted the volatile nature of the regulations, which can potentially force a company to undergo strategic changes with every minor adjustment made. They said, "*If you adjust to one regulation today, maybe next year it is going to change. So go for the strictest and most heavily sanctioned guidelines and, yeah, inspect your risk portfolio,*" (19th of March 2024).

One final factor European companies must consider is the new upcoming regulations that will impact them directly. As our interviewee from CMP15 puts it, "*Most European companies are currently focusing on the new European law that's coming out soon,*" (15th of May 2024). The new data protection regulations have challenged many companies and forced them to rethink many of their prior strategies and develop entirely new ones. Faced with the dilemma of vague and rapidly evolving regulations, companies need to find their own methods to thrive whilst avoiding legal issues and penalties.

Administrative

Besides strategic challenges, administrative challenges were a prominent issue, with companies expressing frustration over the increased bureaucracy and the constant regulation changes.

One potential challenge that impacted companies, was the forced localization of certain processes. As our interviewee from CMP01 noted, "*Usually, the management is heavily centralized in Europe, America, Australia. And the local team in China is just on a day-to-day basis, really administrating the IT systems and IT security. But they are probably not IT experts. So they tend to now localize their IT expertise in order to be able to comply with these new cybersecurity regulations*," (19th of March 2024). To make matters worse, as mentioned in the strategic challenges section, the regulations are also notoriously vague, causing further issues when trying to ensure compliance. This causes further administrative work, requiring companies to continuously interpret and reinterpret the requirements. This difficulty was mentioned by our CMP09 interviewee who stated, "*from what I am aware, there was one major issue in that the regulations were not very precise. They were relatively vague. So, um, many, yeah, it was just very hard to know exactly what the regulations wanted*," (19th of May 2024). Furthermore, companies need to obtain the necessary consent and approvals of their clients to use the collected data. This is a monumental task which should not be underestimated. As our interviewee from CMP10 puts it, "*Basically, the biggest administrative challenge in my opinion has been to receive the consent of the people whose data we process*," (10th of May 2024).

Many international companies have their management centralized in other regions, which makes many decisions harder. As our interviewee from CMP01 puts it, "*The management is heavily centralized in Europe, America, Australia and the local team in China is just on a day-to-day basis, really administrating the IT systems and IT security. But they are probably not IT experts. So they tend to now localize their IT expertise in order to be able to comply with these new cybersecurity regulations*," (19th of March 2024). The rapid implementation of the PIPL has made it harder for companies to properly implement all required aspects in time whilst simultaneously keeping regular operations running properly. As our CMP10 interviewee puts it, "*in the PIPL, this was quite a quick process. I know there have been several drafts. I think the third draft in the end was put into action, if I remember correctly. But it was still quite, quite a short time*," (10th of May 2024).

One final key consequence companies faced involved getting their different departments synchronized. People with different backgrounds will have different views and understandings of certain topics. As our interviewee from CMP17 describes it, "*There are barriers between the people who have a legal background and the technical background people. For technical background people they do not understand the legal but for legal background people they do not understand tech knowledge. So sometimes I think one of the difficulties is to really understand each other*," (24th of May 2024).

Technological

The final category of challenges we focused on were the technological ones. Technological challenges primarily focused on adapting existing IT infrastructure to meet the new requirements. Companies often face significant challenges in this regard.

When it comes to the regulations, sensitive data needs to be handled differently than other types of data. This becomes a massive issue when, as shared by a contributor from CMP11, "*We do not know how to classify certain data,*" (10th of May 2024). Without clear classification standards, teams are unaware of which requirements are applicable. Furthermore, sometimes even requirements are not clear. As our interviewee from CMP12 further describes it, "*the challenge for our companies is to quantify the data. They [companies] own much data. But should they do the process? How much data do they provide abroad, et cetera? Yes. And the last challenge is to do the so-called data mapping mapping. Where do you save the data? Et cetera,*" (13th of May 2024).

In addition to that, there are hardware restrictions as mentioned by our respondent from CMP01, "*regarding, for example, the implementation of the projects, well, you have to accept that with the implementation of these regulations, there is also the imperative that you use Chinese produced hardware or software, for example,*" (19th of March 2024). Many large international companies require their employees to use their private VPN (Virtual Private Networks) to connect to company servers to ensure more data protection. This can, however, become problematic under the regulations, as stated by our interviewee from CMP03, "*In China, you may only use a certified or authorized VPN. And there are only, I think, two providers,*" (5th fo April 2024). Furthermore, companies are also heavily dependent on the compliance status of utilized third-party services or products. If the software they use is non-compliant, their complete operations' compliance can be questioned. This was a specific case mentioned by our interviewee from CMP13, "*For example, SAP or companies who use SAP, They did not have these big issues because SAP was quite quick to implement new, let us say, software structures. Companies who use Salesforce, they had to struggle a little bit more because Salesforce was not so fast to implement all requirements into their software,*" (13th of May 2024). Lastly, although isolating Chinese data in China is a potential strategy, as our CMP10 interviewee puts it, "*Separating IT infrastructure in China is not feasible for certain industries,*" (10th of May 2024).

In order to properly abide by and implement the requirements of the new data protection regulations, companies have faced numerous challenges and will need to continue to do so. They're faced with a wide variety of issues, ranging from strategic, to administrative, all the way to technological. The companies that wish to thrive in these environments need to be prepared to rapidly adapt to changes and face ever-evolving standards, often with significant restructuring required.

5.3.2 Compliance Control

One question our researchers were most interested in, had to do with whether and how often the Chinese government actually assessed the new data protection regulations. This

category, having the overarching topic of control by the government, encompassed several subcategories, such as goals, enforcement, background, regulatory changes, and industry requirements, which will be presented in this order. Given the multitude of sub-topics, each one will be treated individually in the following sections.

Goals

The "Goals" subsection refers to the regulations' intent, as far as perceived by industry members. Their perception on this topic could show if the practical application of the laws added to theory predictions. The results were diverse, resulting in many different codes being identified:

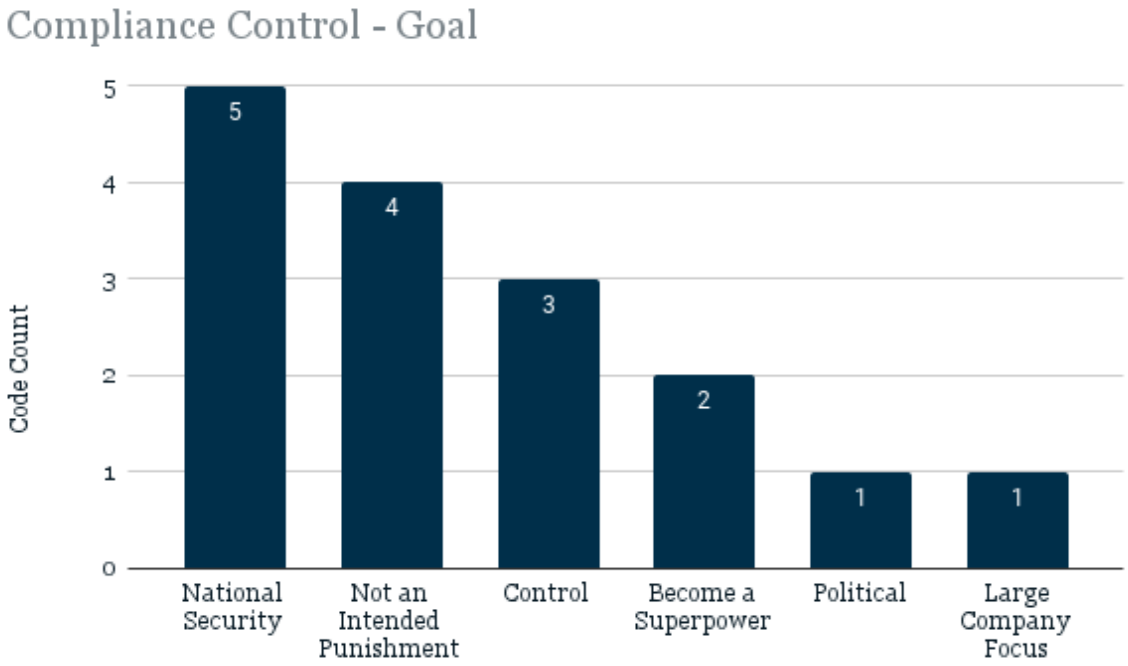

Figure 5.11: Compliance Control - Goal

National Security, along with Control were amongst the most mentioned goals for the regulations. Comments on National Security emphasized its priority for Chinese leadership, as data is seen as an asset that must be protected: *"For the Chinese government as for any other government, data is very valuable. It is a new gold, right? So they are trying to keep the data within China. That is why this is one of the main reasons why there is an increase in new regulations in China to protect data."* - our CMP12 interviewee (13th of May 2024). Control refers to other aspects besides security that the government intended to control. Interviewees mentioned control over foreign companies' growth, political control, and control over the innovation

and regulation balance. The latter was an unheard opinion on the subject, but proved to be logical after the interviewee expanded on the proposition. Increased regulatory control can suffocate innovation and entrepreneurial advancements, as companies must invest internal resources in order to remain compliant. Given the regulations' strictness, it is safe to assume that major actions and costs need to be incurred by companies in order to achieve complete compliance. The vagueness in the regulations allow for a flexible governmental tool to control this balance, tilting the scales to each side as needed. The interviewee CMP06 commented on the government's ability to adjust said balance, "*I think they are pretty good at it [balancing the strictness of the regulation],*" (24th of May 2024).

Another recurring point of interest was that the regulations were not intended to serve as a punitive measure against foreign companies. Some of our contributors highlighted that the regulations were not intended to purge foreign companies, and are similar to their European counterparts' goal to protect personal data. This is even considering the characteristic vagueness, which some believe to be changing: *"I think the trend is not to use it as some tool to make life more complicated, but to try to clarify what it means and who is not affected."* - our CMP16 interviewee (6th of June 2024). In addition to that, it also became clear that the regulations were focused on large, international internet firms, which collect enormous amounts of data, well into the thousands [35]. Similarly to the GDPR, according to interviewees, the regulations were meant to punish companies that acted maliciously towards users' data, by selling or processing it without consent or transparency. The attempt to limit firms' liberty in that sense related closely to another identified code: China's goal of becoming a global superpower. By adding big data and artificial intelligence to its list of "Strategic Emerging Industries List"[21], China has publicly revealed its intentions of becoming a global player in the industry to the extent "*that at one point can overtake the U.S. and can successfully repel a U.S. [cyber] attack,*" - our CMP06 interviewee (24th of May 2024).

Besides the previously mentioned statement, multiple interviewees, including our interviewees from CMP12, CMP06, and CMP11, commented on the regulations' political intent, citing the case involving a large Chinese technology company. According to these contributors, the firm's punishment could have been a backlash motivated by its decision to be listed in New York and allegedly leaking data without consent to the United States. A survey response touches the topic with a different perspective, "*It is important to note that while there seems to be a greater ambiguity in the Chinese regulations, data protection, and security is not only a foreign issue but also concerns local well established Chinese companies, e.g. (censored company name) case!*" - (11th of April 2024).

Background

This sub-category includes data related to background information interviewees believed to be important to fully comprehend the regulatory space in China, with the most mentioned topic being culture. Two contributors elaborated on the cultural difference (compared to Europe), saying that strict requirements are normally set first in order to shock, communicate

severity and ensure compliance. "*A gradual implementation does not work often here. It is either full throttle or it is full brake and nothing in between. And that, in my personal opinion (...) the what [is implemented] is good, the how [it is implemented] could be better, but that is China,*" - CMP10 (10th of May 2024). Afterwards, regulations are slowly adapted and adjusted to better support the market. *"In many ways China is more market oriented than a country like Germany. (...) But in China it goes the other way. They always let people develop and experiment and then only at a later point, [jump in and take control]*" - our CMP06 interviewee (24th of May 2024).

Furthermore, the importance of economic and geopolitical context was emphasized by two contributors (CMP06 and CMP13). The first mentioned the exporting dominance in the Chinese economy and how having an international-peer data protection regulation could ensure that Chinese products fulfill international standards. The second elaborated on how uncertain geopolitical contexts play a great role in such regulations. Uncertainty over other nations creates the need for self-protection and, in turn, stricter laws. Said observation cooperates with another comment, stating that the regulations did not catch industry members by surprise, as it was "*a long conversations with large market players pointed towards new regulations as early as 2019,*" - our interviewee (CMP13 - 13th of May 2024).

Enforcement

Understanding how the regulations were being assessed by Chinese authorities in practice was also an important research topic. Responses here were extremely divided. Whilst some interviewees mentioned office raids, frequent audits (especially in certain regions), totalitarian practices by authorities, approval requirements, and a general increase of enforcement, others mentioned a lack of enforcement and assessment efforts, government aid in successful regulatory transition, loosening of the regulations and even open negotiations with authorities. Said duality can be seen in the following two responses: "*the local authorities, not the the cyber administration so far, but local authorities come often to company audits. In the area where we are located that was checked by the environmental health and safety authorities over two hundred times in one year,*" - our CMP10 interviewee (10th of May 2024); "*Actually, you know, that is always the thing, because there are always a lot of rumors that in China, sometimes it is hard to follow the regulations, so if you do not do it, you can not do it. You need to pay huge fines, or you are personally responsible, or something like that. That is maybe not wrong, but this happens not too often,*" - our CMP13 interviewee (13th of May 2024).

Although the mentioned duality complicated the coding of this section, it provided insightful analysis results when combined with results from other sub-sections, which can be seen in the Analysis chapter 6.

Industry Restrictions

This subsection encompasses all mentions of industry-specific regulations, an aspect of the law triad that appeared in some interviews and literature. We identified four codes: Longer

Deadlines, Higher Standards, Higher Data Sensitivity, and Clearance Requirements.

Theory on the topic stated that specific industry segments were under stricter rules [36]. Let that be because they collected or produced sensitive data. Industries such as automobiles, infrastructure, military, finance, or telecommunication also faced higher standards, such as the explicit need for security clearance in order to transfer data abroad [37]. Furthermore, business models also seem to influence how quickly companies must comply. Our CMP15 interviewee shared: "*B2C companies sent in their documents in February of last year [2023] whilst B2B companies sent theirs in by the 1st of December [2023],*" (15th of May 2024).

Regulation Changes

The final subsection in compliance control referred to the most recent regulatory changes. Three main changes were mentioned. The first relates to a softened cross-border data transfer standard. On the 23rd of March 2024, the Cyberspace Administration of China (CAC), China's central cybersecurity and data protection authority, published the „Provisions to Facilitate and Regulate Cross-Border Data Flow", which eased the cross-border transfer for enterprises that transferred employee data and customer data of less than a hundred thousand data subjects [38]. However, the interviewee who raised the topic commented: "*In my opinion, it is quite unfortunate that you first set a bar like that, and basically everybody's trying to fulfill the bar. Then afterwards, I think two years later, basically after the law became effective, you lower that bar. It led to quite some challenges,*" - our CMP10 interviewee (10th of May 2024).

Lastly, many mentioned the vagueness present in all three laws. Several contributors including CMP14 and CMP16, mentioned that they are slowly being clarified.

5.3.3 The Role of a Data Protection Officer

Finally, as the GDPR already mandates larger companies to have a Data Protection Officer (DPO) we were curious about how the new regulations affected their roles. Multiple questions surrounded the topic, specifically whether new roles were introduced or if the preexisting DPOs were given more tasks and responsibilities.

40% of interviewees who responded to the question shared that they did not have an official DPO position filled. Half of them mentioned having a lawyer who acts as a DPO, as in the following comment by our CMP12 interviewee: "*We do not have a designated DPO. But we have data protection specialists, lawyers who basically serve as a DPO, but it is not an official position,*" - (13th of May 2024). The other half mentioned that the role's responsibilities were overtaken by other positions, such as in the case of our CMP02 interviewee: "*We have an IT guy who takes care of our personal data that is saved on our company server and our company cloud. But, it is not like a big department or special officer,*" - (25th of March 2024).

However, there were some differences in how the position was filled. One shares that "*We have a DPO assigned in China. A Chinese citizen with cross function with the German department.*

We have meetings every week and it's a special role,"(CMP15 - 15th of May 2024). Another shares a different situation, saying: "*We have one within the group who was sitting in Europe. But he is not very willing to take over that function for China*," (CMP10 - 10th of May 2024). This interviewee explains that they ultimately decided to outsource a specialist for the role, who will then monitor the company's compliance levels towards the laws. Similarly, an interviewee (CMP18 - 4th of June 2024) hired a consulting company that provides a service similar to the DPOs'. Another contributor (CMP09 - 19th of May 2024) mentions that the role was already filled before the regulations, as the GDPR already set that requirement; however, he adds that after the regulations came into effect, such roles had to reevaluate their responsibilities to include Chinese-specific requirements.

5.3.4 Impact on Small and Medium-Sized Enterprises

A surprisingly great amount of mentions of Small and Medium Enterprises, or SMEs, for short, motivated the research team to create a separate category just for these contributions. No subcategories were identified as the category itself was already sufficiently narrow. Furthermore, no sufficiently large overarching titles were found when analyzing the contributions. Before presenting the results, it is important to establish a clear definition of SMEs. The research team utilized the definition provided by the European Commission [39], which states that micro, small, and medium-sized enterprises are defined by staff headcount (limited to ten, fifty, and two hundred fifty respectively) and turnover or balance sheet (limited to two million euros, ten million euros, and forty-three million euros respectively).

With a total of ten contributions related to SMEs, they paint a full picture of SMEs' perspective on the topic. Our CMP16 interviewee sets the stage, stating that, "*the majority of companies who are operating here in China, they are smaller or medium sized setups. And for them, well, they are in the process of adjusting*," (6th of June 2024). However, although SMEs occupy a large portion of the Chinese market share [29], the regulation's intent of specifically targeting "large internet providers" [35], as previously mentioned in the enforcement goals section, is overwhelmingly supported by this section's contributions, as in: "*But we are, as a small company or small organization, we never touch the shareholder to this law. So we are not familiar. Descriptions are the big company's situation because yeah, we focus on our industry sector and do not handle much personal information*," - our CMP05 interviewee (15th of May 2024). The support for this statement continues, with four contributions stating that SMEs were less affected than large corporations. The following contribution by CMP13 was clear: *"It [cross border transfer] is not so complicated like a lot of people saw. Only for very big companies. If you are, let us say, you have more than a hundred thousand users, of course, that is another thing, but for normal companies, especially SMEs, large to medium sized companies, I think it is not a big topic at all*," (13th of June 2024).

In counterpart, however, another interviewee reassured that SMEs are not outside the regulations' scope and should still be working towards compliance. A task that is not easy considering the topics raised by our interviewee from CMP13: resource limitations. This

contributor highlights that especially smaller enterprises normally do not have the resources to first understand requirements, assess current compliance levels, and ultimately adapt. The result, as stated by our CMP16 interviewee, is: "*How should I, with my small setup here, comply with all of that?*" (6th of June 2024). Our results indicate that SMEs either felt relaxed, believing to be below the thresholds, or overwhelmed, being unsure if they were able to comply with requirements and involved costs.

The duality in responses here reaches its climax with this last contribution by our CMP16 interviewee, who stated that the regulations pose a greater challenge, especially to SMEs: "*The smaller the company gets, the more challenging it is, I think, to really comply. It is not only data protection. There are regulations in all ways: where the company is active, supply chains and many, many regulatory aspects they need to be aware of,*" (6th of June 2024).

5.3.5 Comparison Between the GDPR and PIPL

The final topic, directly covered in interviews, was concerning the specific differences between the GDPR and the PIPL that the interviewees may have noticed or experienced. Here we wished to determine by how much the new Chinese data regulations deviated from preexisting standards such as the GDPR or how similar they may actually be.

In this case, there is no need to subdivide the category further, as all the different views were quite harmonious. A relatively common consensus ended up being that the GDPR and PIPL are fundamentally very similar and only differ in minor aspects. As our CMP01 respondent noted, "*It is [GDPR as the basis for the development of the Chinese regulations] more like a copy-paste approach here. The Chinese have acknowledged that the Europeans did a good job,*" (19th of March 2024). These differences usually boil down to cultural differences and the fact that the GDPR has had much more time to develop and, thus, much deeper foundations. One respondent from CMP17 highlighted, "*GDPR and its specifications, regulations, explanations have really good practical guidance for companies to follow,*" (24th of June 2024). Although both regulations require responsible data handling, China additionally requires that important data to be stored locally. Our interviewee from CMP10 adds, "*In Germany, the mindset is responsible data handling, and you are fine. Here in China, it is more like handle the data responsibly and save it in China, and you are fine,*" (10th of May 2024).

Multiple interviewees mentioned how, in the EU, the residents tend to feel more entitled to their data and how it is used. Our interviewee from CMP11 explained, "*In the European Union, the general point of view of the Europeans is that I am a consumer, so I should have rights and be paid for my data,*" (10th of May 2024). According to the interviewee, Europeans care significantly more about protecting personal information as our interviewee from CMP17 also observed: "*In the EU, I think it is more about not disclosing people's religions or sexual orientation,*" (24th of May 2024). A further contribution by our respondent from CMP11 is, "*In China, and not only in China, in Japan, in South Korea, Singapore, and some of the other Southeast Asian nations, it works more like an asset and as long as it provides me convenience, I am willing to accept it,*" (10th of May 2024). Expanding on these insights, our interviewee from CMP10 pointed out, "*I think that*

the most significant difference (...) is that you need the consent for cross-border data transfer, and the GDPR, as far as I know, does not have that regulation in any way," (10th of May 2024). The difference in disallowing cross-border data transfer is one of the foundational reasons behind a significant portion of the disadvantages mentioned in prior sections.

Regarding the complexity of the regulations, the GDPR has existed for a longer period of time and has had its time to properly integrate into existing systems as well as develop comprehensive and refined guidelines. Our interviewee from CMP17 stated that the "*GDPR and its specifications, regulations, explanations have really good practical guidance for companies to follow,*" (24th of May 2024).

In certain interviews, we also encountered cases where they did not notice the differences as much. In these cases, by having a preexisting system in place to handle the GDPR regulations, implementing the new data protection regulations was relatively simple. Our CMP18 interviewee, for example, mentioned, "*As both regulations are somewhat similar, it was relatively simple to adjust our strategy to them,*" (4th of June 2024). In contrast to that viewpoint, a survey respondent from CMP20 shared, "*One of the biggest challenges remains the simultaneous implementation of PIPL and GPDR as we process data subjects from both jurisdictions and regulations in terms of storage etc., they sometimes contradict or at least require inefficient redundancies,*" (20th of June 2024).

Moreover, the primary objectives of these regulations differ slightly. Whilst the GDPR has a larger focus on individual rights, the PIPL places more emphasis on governmental control and security. As our interviewee from CMP12 puts it, "*The goal of GDPR is to protect personal data of the individual (...) the primary goal of the Chinese regulation is to protect data for the Chinese government,*" (13th of May 2024).

Overall, the interviews reveal that while GDPR and PIPL share a common foundation in promoting responsible data handling, their differences are partially shaped by cultural differences, their respective regulatory development stage, and strategic goals. Understanding these differences will help you better understand the compliance landscape.

5.3.6 Prediction Comparison

In the last section before proceeding with interpreting our findings in the analysis chapter, we will compare the gathered results with our prior predictions.

As previously mentioned in the methodologies section, SP1, 'The response rate to email (or other) inquiries will be low (5-10%), especially from companies that might not yet be fully compliant,' was significantly more impactful than we could have predicted. The response rate to emails was a meager 2%. Thankfully, this could be counteracted by using other platforms and personal connections (with a combined response rate of 44%), increasing total response rates to 6,9%. Regarding the second part of this prediction, 87% of our interviewees mentioned being well-established in the market.

SP2, 'Sourcing companies will be difficult, as data compliance can be considered sensitive information to share. Few companies will feel confident in sharing it,' was indirectly hinted towards by participants CMP05, CMP15, and CMP18 as they were unwilling to have the interview recorded, specifically stating either not having the necessary permissions to allow the interview to be recorded or wishing to avoid any potential backlash. Although it is impossible to estimate how many recipients rejected or ignored our invitation due to the sensitive nature of the information being dealt with, we can assume it had an impact.

Regarding SP3, 'Individual employees may feel they lack permission to participate in an interview as a company representative,' our fears were confirmed as one of the specific rejection reasons we received: "*I have checked the questionnaire, and what is needed is my assessment of my employer's data protection status. I am afraid I will not get permission to disclose the company data protection maturity level, even though you mentioned it would be anonymous and for study purposes, sorry,*" - contact attempt via networking platform, adapted for anonymity (15th of May 2024).

IP1, 'The validity of certain statements may need to be scrutinized further for all companies that choose to stay anonymous (fewer repercussions/traces for lying),' ended up being unnecessary, due to the fact that all our interviews were conducted anonymously. The original concerns of this prediction were, however, one of the main reasons behind how we structured our interview script. The first section analyzed the interviewees' general understanding of their respective companies and the data protection regulations. With this combination of details and information gained from prior interviews, we could deduce the rough direction our interviews would take and the information provided. This helped us trust and validate the validity of the information gathered.

The prediction RI1, 'Companies will be skeptical about future operations in China,' was accurate to a certain degree. Our interviewee from CMP03 states, "*As I also mentioned in the beginning, this uncertainty, nobody likes,*" (5th of April 2024). Without certainty, companies will always need to be wary and overly cautious. Over time, it has become clear that companies are exempt from data transfer requirements "*if the transfer is necessary for performance of a contract or cross-border HR management, or the volume of personal information (PI) transferred is below a hundred thousand individuals*" [40]. As the interviewee from CMP03 expressed: "*I am below this threshold, so I do not have to worry anymore,*" (5th of April 2024). Consequently, many companies are adopting a wait-and-see approach, carefully evaluating the risks before deciding how to proceed with future investments and expansions in China.

Regarding CS1, 'Very few companies will directly admit to not implementing the new regulations as it can result in potential backlash from China and the media,' which is an aspect that we could not assess. As our interviews were all conducted anonymously, we could hopefully mitigate the potential impact of this concern. This, however, does not prevent the possibility that only interviewees from compliant companies will be willing to participate in the interviews. Furthermore, as most contributors assured being fully (or mostly) compliant with the requirements 5.3, only made it harder to judge the impact of CS1. Only in the case

of smaller companies, such as in the case of CMP02, did we hear comments such as "*We did not do anything*," and "*Maybe there is something that we have to take care of as a foreign company*," (25th of March 2024).

CS2, 'Companies that do not wish for anonymity will likely have implemented everything as required,' was able to be entirely mitigated, as noted in the methodologies section. By keeping all interviews anonymous, biases between anonymous and named companies were impossible.

EC1, 'Chinese authorities can abuse access to intellectual property or confidential information.' Some interviewees expressed apprehensions about the implications of the new regulations on data security, and the potential access authorities would have to sensitive information. The interviewee from CMP08 noted that, "*there could be some sort of protectionism where they gather the data about outside competitors and use that to facilitate the growth of internal counterparts*," (20th of April 2024). As the interviewee from CMP18 states, "*One of our greatest concerns is IP protection*" (4th of June 2024), and thus, their primary concern is how these new regulations might result in their IP being used without their consent.

EC2, 'Companies will feel overwhelmed by compliance rules, having to comply simultaneously with multiple data protection regulations worldwide,' naturally resulted in companies prioritizing the regulations that would impact them the most. As stated by the interviewee from CMP15, "*Most European companies are currently focusing on the new European law that is coming out soon*," (15th of May 2024), as those regulations will impact them more directly. Thus, their focus on international regulations, such as the PIPL, will slightly suffer.

EC3, 'Security of employees, as authorities may hold individuals personally accountable for their company's non-compliant status,' was noted as a serious concern by the interviewee from CMP11 who went on to tell us about a specific case: *"He [a colleague] shared this publicly available research that can be found on Baidu. He copy pasted the link and sent it to the (...) [country] [client] company. The (...) [country] company reviewed it and found it to be fantastic information. National security then comes in and asks: why did you share such information?*" (10th of May 2024). Judging what can and cannot be considered sensitive data becomes challenging with these precedents.

CC1, 'Companies will have to rethink their investment strategies regarding existing and future projects in China,' is not directly supported or denied by the interview responses, however, this changes once we expand the premise to include rethinking strategies in general. Our interviewee from CMP18 noted the impact of the new regulations, stating, "*The usage of global platforms, such as HR, makes it difficult to comply with so many different regulations across the globe simultaneously*," (4th of June 2024). This showcased some strategic adjustments, and changes companies must make to align with the PIPL, CSL, and DSL. Our respondent from CMP10 mentioned, "*The biggest issue was that my colleagues, who are all Chinese, did not take it very seriously, which is also understandable because, again, the way the law works here is a little bit different*," (10th of May 2024). This indicates that cultural differences also increase the challenge, and thus, companies need to adopt new strategies to ensure compliance and adherence to

local practices and regulations. Furthermore, an interviewee from CMP14 described strategic communication challenges, noting, "*There are a lot of strategic discussions at the moment. As there always are, but in the last few years (...) it was difficult or even more difficult than before to maintain efficient communication,*" (1st of June 2024). This supposition is also confirmed by AHK's flash survey on the topic, with 53% of respondents planning increasing their investments in the next two years [41]. These responses confirm that companies need to significantly rethink their current strategies, including potential investments in China, as there is a need to adapt to new regulations, address cultural differences, and improve internal communication to successfully navigate the ever-complex regulatory environment.

CC2, 'Financial burden, as new regulations, can be time-consuming and financially taxing,' is strongly supported by the interview responses. An interviewee from CMP01 pointed out the constant changes necessary, stating, "*If you adjust to one regulation today, maybe next year it is going to change,*" (19th of March 2024), indirectly emphasizing the constant resource drains caused by the demands. Another respondent, the interviewee from CMP10, mentioned, "*We have to do regular training, and we have to develop the training,*" (10th of May 2024), highlighting another area requiring continuous financial and time investments to stay compliant. An administrative burden was emphasized by our interviewee from CMP09, who noted the vagueness of regulations, stating, "*The regulations weren't very precise. They were relatively vague,*" (19th of May 2024), which leads to additional costs for the necessary legal consultations and the resulting actions that need to be taken in order to stay compliant. These responses indicate that the new regulations significantly increase the amount of necessary financial and time commitments required from companies, confirming the prediction that the regulations are both time-consuming and financially taxing.

Although not always the case, CC3, 'Companies are either planning great restructuring within their Chinese sectors and services or planning to shrink their participation in the market,' was accurate for some firms. One interviewee from CMP07 noted aspects such as: "*Localizing some management, kind of isolating, the Chinese branch from the European branch so that they have more flexibility to comply with the regulations,*" (19th of May 2024), highlighting the significant restructuring already done as well as the indirect decline of their international influence on the Chinese market. The interviewee from CMP10 noted similar restrictions, stating, "*We cut off certain data transfers from our local HR system into the global HR platform,*" (19th of May 2024). These responses indicate that China's tightly controlled regulatory environment is forcing many companies to substantially change their currently implemented structures to meet compliance requirements while often reducing their international influence. The interviewee from CMP10 further highlights: "*The costs to remain compliant increased, and for us, it was still quite slim with our IT infrastructure. For other companies, it might be a much bigger issue, which can even lead to a company having to decide to leave the Chinese market in the end, especially if they are talking about large-scale user data being saved abroad. On the other hand, I would also say the company was not listening to the market developments because the first tendencies were already visible since 2017 with the cybersecurity law,*" (19th of May 2024).

P1, 'Companies will find it more difficult or resource-consuming adapting to the PIPL

compared to the GDPR,' is quite a divisive topic when looking through the interview responses. On the one hand, an interviewee from CMP01 noted, "*If you adjust to one regulation today, maybe next year it is going to change,*" (19th of March 2024), highlighting the constant need for adaptation and the associated resource demands. Another respondent emphasized the rapid implementation of the regulations and the resulting challenges it brought, stating, "*and in the PIPL, this was quite a quick process. I know there have been several drafts. (...) But it was still quite, quite a short time,*" (our CMP10 interviewee - 10th of May 2024). This rapid rollout and the PIPL's stringent requirements forced companies to invest heavily to stay compliant. In contrast, the GDPR's further developed framework provides clearer guidance for companies. These factors make the PIPL, the DSL, and the CSL considerably more challenging and resource-intensive to comply with. On the other hand, multiple interviewees had completely different views on the topic. For example, our interviewee from CMP05 stated, "*In my opinion, for smaller German companies, there is a higher cost for complying with the GDPR,*" (15th of May 2024). Our respondent from CMP14 mentioned, "*For us as a company, not really. We have not seen differences in complying with the PIPL and the GDPR,*" (1st of June 2024). Additionally, CMP11 noted, "*But when it comes to the cross border data transfer, thanks to the knowledge that I obtained through GDPR before, I was able to do the data classification and then do all the data mapping and all this kind of stuff,*" (10th of May 2024), suggesting that prior experience with GDPR helped facilitate compliance with PIPL. These two sides showcase the multifaceted nature of the results from our interviews, where numerous factors always needed to be considered. In this case, factors such as the company's size and prior existing systems built to comply with the GDPR had the most impact.

Our P2 prediction, 'Companies will mention the lack of clearness in the PIPL compared to the GDPR,' was proven by the interview responses, which consistently highlighted the ambiguity and vagueness of the PIPL. For instance, our interviewee from CMP09 noted that the regulations were "*relatively vague,*" (10th of May 2024) as well as difficult to interpret, while our interviewee from CMP03 expressed concerns over "*misinterpretation and misunderstanding,*" (5th of April 2024). This lack of clarity forces companies to adopt a cautious approach, often leading to increased operational costs and the need for frequent legal consultations. In contrast, the GDPR, with its well-established guidelines, provides a noticeably clearer framework to ensure successful compliance. This discrepancy ensures significant challenges for companies adhering to the new Chinese data protection regulations. It substantially impacts their strategic decisions and often results in a wait-and-see approach where companies must await future, more precise definitions and guidelines.

The predictions ended up being an extremely useful tools to avoid biases as well as target specific preconceived ideas gathered from literature. They were a vital part of the foundation that enabled our interviews and data gathering process to be successful.

6 Analysis

With the results from the previous section, we now had quantitative data at our disposal. This section will dive deeper into the insights generated by said data. By analyzing trends and possible correlations within our collected data, we can infer possible answers to how the PIPL, DSL, and CSL affected foreign companies in China. However, before presenting our findings, we would like to first compare our results with the foundational literature used for our research.

6.1 Literature Comparison

Our literature review laid the foundation for us to confidently conduct interviews and collect data on the impact of China's new data regulation laws. During the literature review, we focused on the law's intricacies, comparisons with other global regulations such as the GDPR, and the strategic changes they forced companies to undergo. After concluding our interviews and analyzing the results, we can verify that our empirical coding results closely match what we learned from the literature. Specifically, our results showcase the significant challenges and strategic shifts companies faced and had to undergo under these new regulations.

The literature often pointed towards the need for companies to rethink their strategies to comply with new regulations such as the PIPL. For instance, in their article, Yvonne Lau [11] pointed out that the additional requirements and regulations enforce the need for data approval and storage rules, which our interviewees confirmed. An interviewee from CMP06 listed multiple large international companies that "*were all forced to build a completely new infrastructure, everything local,*" (24th of May 2024). Our interviewee from CMP10 further states, "*The mindset in Germany is: handle the data responsibly, and you are fine. And here in China is: handle the data responsibly and [, additionally,] save it in China,*" (10th of May 2024). Our CMP15 interviewee verified the need for approval, "*We applied for approval from the Chinese government and received a paper-stamped approval,*" (15th of May 2024). Our coding results also reflect the need for a shift in strategy, with interviewees noting the need to adapt IT infrastructure as well as operational procedures, such as mentioned by our interviewee from CMP03, "*a lot of people that bring their whole IT infrastructure into China and keep it within China and avoid sharing the data IT infrastructure abroad,*" (5th of April 2024). This was consistent with Lau's findings [11] on the regulations' demands.

Furthermore, the work by Samm Sacks and Manyi Kathy Li [12] highlighted the vagueness of the PIPL, suggesting it could be used to favor national companies and give the Chinese

government the flexibility to enforce the laws as desired. This aligned with our coding results, where multiple interviewees noted the lack of clarity and the constant need to interpret new and changing regulations. Our CMP10 interviewee mentions, "*in March, (...) some of the legal regulations were softened up again,*" (10th of May 2024). The volatile aspect of the regulations was also mentioned by our interviewee from CMP01, who stated, "*If you adjust to one regulation today, maybe next year it is going to change,*" (19th of March 2024). Our empirical data confirmed the theoretical strategic consequences identified in the literature, including the need for companies to allocate more resources to ensure compliance.

The article "How China's data privacy and security rules could impact your business," by Ernest Young's Chi Chen and Leo Zhao [18], together with PwC's "10 ways China's new data rules will change your business" [19], highlight the substantial costs associated with compliance, especially for heavily targeted industries [36]. Our coding results have revealed that companies often need to invest heavily to stay compliant. This includes restructuring their local data infrastructure and other cost sinks, which increases financial burdens. This view is shared by many of our interviewees, including our interviewee from CMP07, who states, "*Everything I said so far, HR, the technological changes, all that costs a lot. But it also requires a lot of time, which could be better spent doing something more related to our purpose and goals as a company,*" (19th of May 2024). This mirrors PwC's literature's [19] depiction of the new regulations' economic impact and the necessity for companies to evaluate their strategies regarding their future participation in the Chinese market.

The coding results we gathered and analyzed from our interviews provide empirical support for the insights and predictions stated in the existing literature resources. Due to China's new data protection regulations, companies face significant strategic, operational, and financial challenges. The combination of results of the existing literature, in combination with our empirical findings, emphasizes the massive impact of the combination of the PIPL, CSL, and DSL on international companies operating in China, necessitating substantial restructuring and continued vigilance to successfully navigate these complex regulations.

6.2 Findings

6.2.1 The Impact of Industry, Knowledge, and Company Size on Regulatory Views

Analyzing the collected data, the research team noticed that of all interviewed companies, 8% view the regulations negatively, 24% view the regulations positively, and 52% view the regulations neutrally 5.5. Larger and more established companies tended to have a more neutral (8) and sometimes positive (4) perception of the regulations. Small and medium companies were more evenly distributed among the 4 categories 6.1. At the same time, there was evidence to suggest that interviewees with medium familiarity viewed the regulations more negatively (2), with 0 of them having a positive position. Furthermore, companies with higher familiarity with the regulations, such as law and consulting firms, tended to have more positive (5) or neutral (7) views of the regulations 6.3. That is probably because law

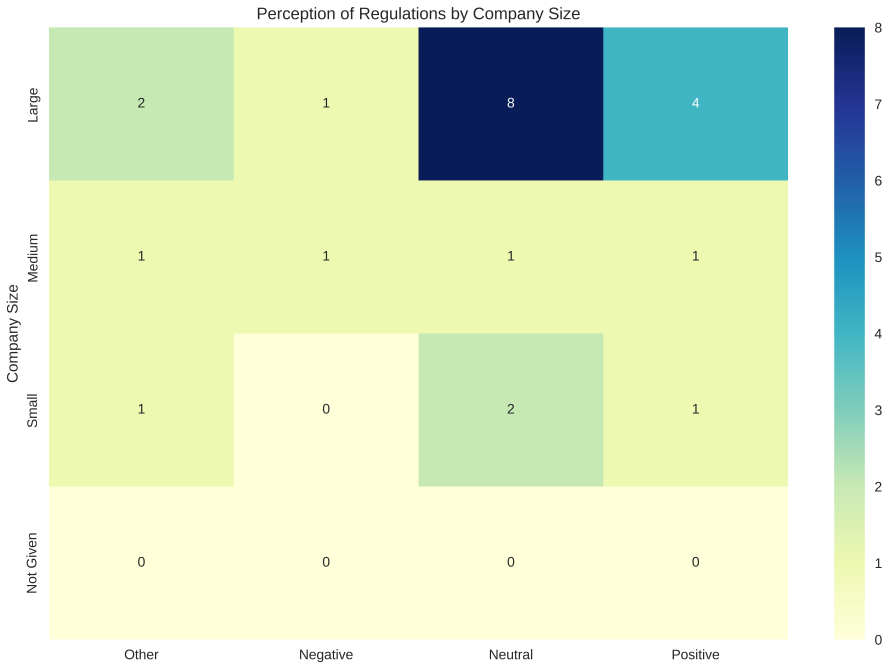

Figure 6.1: Perceptions of Regulations by Company Size

and consulting professionals could thoroughly name both positive and negative aspects of the regulations and still recognize their importance in regulating Chinese cyberspace. The interplay between these variables is depicted in graphs 6.1, 6.3, 6.2.

Based on the observations, the research team concluded that, although the regulations focused on "internet platform services" [35] are being adapted to ease enforcement for SMEs [34], as of currently, they cause concerns among this group. This conclusion is logical, given that larger firms have more extensive human and internal resources to prepare, plan, and adapt accordingly. In contrast, smaller enterprises face multiple challenges due to limited resources and smaller legal teams. These teams must first understand and adapt to the regulations, with overwork as a real risk. Most interviewees who shared being overwhelmed, anxious, or uncertain were from SMEs, as seen in 6.1, where four interviewees mentioned not having a clear position on the topic.

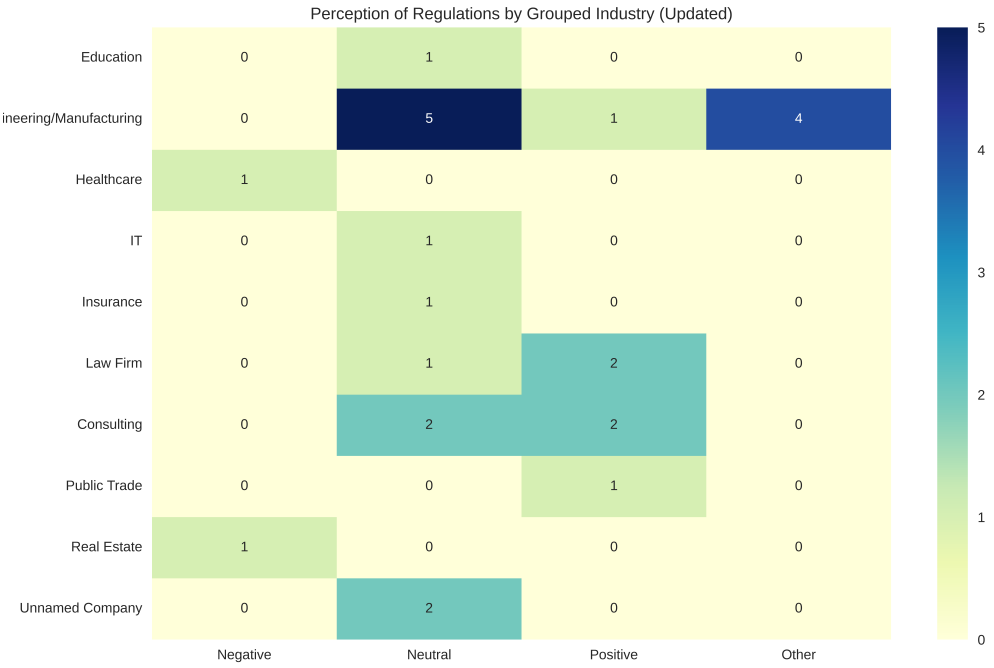

Figure 6.2: Perceptions of Regulations by Grouped Industry

Therefore, the research team identified the following topics necessary for all foreign companies operating in China, but especially SMEs. Firstly, companies must bridge the knowledge gap, investing their resources not to fully grasp the complex regulations but to conduct a self-assessment, identifying if the company is under given thresholds or other exceptions [40]. Specialized consulting firms can also conduct assessments, depending on the complexity of internal processes. Secondly, the realization that the regulations are not intended to unjustly punish foreign firms is becoming more apparent. Realizing this aspect is essential, as multiple interviewed experts mentioned, and the processes involved are much simpler than those that are publicly perceived.

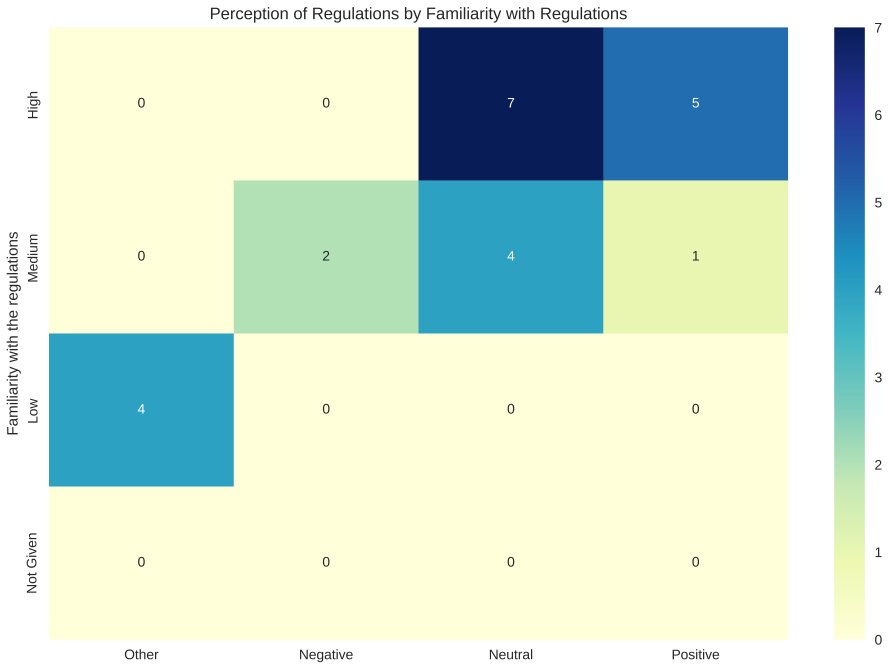

Figure 6.3: Perceptions of Regulations by Familiarity

An additional conclusion was that non-legal experts' law requirements are still unclear. Predominantly, law firms and consulting firms expressed favorable positions on the law (four out of seven, and zero negative positions). For instance, they mentioned that the laws were either clarifying, necessary, or positive. At the same time, multiple interviewees (including lawyers and experts) shared that they found the regulations to be complex and required time and resources to be comprehended. Its complexity seems to derive from two main aspects: First, the multi-area skill set required from lawyers, as stated by interviewee CMP16: "*I think this complexity of different kinds of expertise that you need is legal I. T. Bringing them together combined with the fact that this is all new and very technical is the biggest challenge to implement anything now*" (CMP16 - 6th of July 2024)". Second, the regulations' vagueness, which seems to be changing, as new efforts by the authorities attempt to clarify and loosen the cyberspace laws[34]. The prior, however, is a particular challenge for small and medium-sized firms. Consulting and law firms can hire multiple specialized lawyers, while other companies need diverse legal services, making specialized lawyers a necessary cost. Our results show that 4 out of 6 mentions of recruiting and outsourcing came from these companies.

It was not until the middle of our interview process that one contributor shared via email that the German AHK (Chamber of Commerce) in China had surveyed the topic in May 2024, months after our research started and the intense literature examination in our research

was concluded. The survey [41] focused on cross-border data transfer compliance but also captured other relevant observations on the discussion. After acquiring this information and examining the survey's results over 186 companies, we identified the opportunity for cross-examination with our own results, especially those in this subsection. Unfortunately, the survey did not disclose respondents' categorizing variables, so further examination of some of our hypotheses remains open. 29% of the survey's respondents advocated for a more transparent regulatory environment, confirming our conclusion that the regulations are still unclear for some industry members. Simultaneously, 47% of respondents mentioning concerns about equal treatment of foreign and domestic companies were not identified in our research results. Our interviewees' contributions mostly attempted to state the opposite: the laws were not a tool against foreign companies, as in: "*I do not think that China is strengthening its cyber security laws and regulations to go after foreign companies now, that does not mean you should not be careful and be compliant does not mean you should not pay for my reports*," (CMP06 - 24th of May 2024). However, there were interviewees that confirmed the survey's results: "*from the perspective of the foreign companies doing business in China is getting more and more difficult, right?*". Furthermore, 61% of respondents mentioned price pressure as a dominating challenge. Our results also show great concern regarding costs, which could pressure prices 5.2.6. Lastly, another takeaway by the AHK was that 53% of respondents planned to increase their investment in China in the coming two years, down from 61% in 2023. Although our research did not question interviewees in that regard, this result could potentially represent a reflection of the recurrent mention of uncertainty in our results 5.2.

6.2.2 Strategic Planning: A Framework for Compliance

To address the uncertainty surrounding the regulations, the research team combined literature insights, collected data, and identified a framework that could serve as a guideline for companies tackling this challenging scenario. The importance of strategic planning for companies planning to operate or already operating in China cannot be overstated.

The research team identified three main steps in how planning should be conducted around the topic. First, there is risk assessment. Companies evaluate their risk level based on the processed data's sensitivity, the company's industry type, and the amount of collected data. Common strategies here were consulting a specialized company, a compliance officer, or IT teams. These approaches might be challenging for smaller firms but are an option for medium and larger companies. One of our interviewees provided an example of this step's result: "*That was then from the point of view of our group not enough. We hired an external lawyer who, who additionally supported us in there in the analysis of all of these laws and where we stand at and had a local implementation project where we tried to make sure to get all of the things done, like the impact assessment.*" — *our CMP10 interviewee* (10th of May 2024).

The second step is prioritization. Given the regulations' complexity and large scope, companies can feel overwhelmed (as seen in the 5.3 section). This is why companies need to include a selection of the most critical requirements in their plan. Furthermore, considering

the potential for future legal changes, choosing the most stringent requirements minimizes the risk of redundant work and resource wastage.

"*If you adjust to one regulation today, maybe next year it will change. Go for the strictest and most heavily sanctioned guidelines and, yeah, in respect to your risk portfolio,*" — our CMP01 interviewee (19th of March 2024). This statement points towards the third step: resource allocation. After identifying their risk level prescription from the laws and prioritizing the most important requirements, companies need to manage their internal resources to assess and comply with higher legal risk requirements. A considerable amount of resources need to be allocated for these complex tasks, as noted by the following two interviewees: "*(...) you have to implement all the necessary changes. And it is just a massive amount of cost. (...) restructuring costs, human resources, IT, and so on,*" — our CMP09 interviewee (19th of May 2024) and "*A lawyer can only process things when he knows what he should process, so we spent many internal hours on the topic. If it were just a ballpark number, I would say something between 100 to 200 hours, and that is often also on director level and above, so really top management resources in the end,*" — our CMP10 interviewee (10th of May 2024).

The research team identified key factors that appear to play a large role in determining how severely a company will be affected:

1. The requirements will be stricter if the industry type is part of the sensitive industries list [37].
2. Understanding a company's operational requirements is important when it comes to how companies approach data localization. For instance, determining whether low or high latency is required allows for greater flexibility in choosing data localization options: "*depending on what kind of industry, for example, internet or things, industry 4. 0, they need better frequency, lower FPS, so they tend to go to Singapore or Hong Kong, but for example electronics or just yeah, dealership locations in China, they do not need this high frequency, so they go back to Hong Kong,*" (our CMP01 interviewee - 16th of March 2024).
3. Business model and company size. Our research indicates that SMEs in the B2B sector were the least affected by not dealing with sensitive information and handling amounts of data below the defined threshold - "*It [the regulations] is basically not very relevant to us since we are not in a critical infrastructure. So we are a B2B business and again, not for critical industries*" (CMP10 - 10th of May 2024) and "*B2C companies sent in their documents in Februrary of last year whilst B2B companies sent theirs in by the 1st of December*" (our CMP15 interviewee - 15th of May 2024).
4. The position in the supply chain. A special statement regarding the research process emphasized that businesses at the end of the supply chain must evaluate compliance from components, resulting in a complex internal compliance assessment - "*OEMs (end of supply chain) are strongly hit because you have to make sure that all the product or services used so far comply with they are all compliant*"(CMP18 - 4th of June 2024).

The strategic planning framework can be summarized in the following steps: risk assessment,

prioritization, and resource allocation. Additionally, companies are especially exposed to risks if they fall under the following criteria: is a business-to-consumer (B2C) company, provides services requiring low latency from servers, large companies (handling data beyond or close to the defined thresholds), are located at the end of the supply chain, or are part of a sensitive industry.

6.2.3 Cultural Influences on Regulatory Compliance

Our next observation was the importance of culture in data protection compliance. In various aspects, culture has played a role in shaping the regulations and how companies interact with the laws. Culture as a leading factor for the regulations' profile and characteristics was extensively mentioned in our data: *"A gradual implementation does not often work here. It is either full throttle or full brake and has nothing in between. That is China,"* (our CMP10 interviewee - 10th of May 2024) and "*In China, if nobody is looking after you or pushing you, then you will more or less ignore it,*" (our CMP03 interviewee - 5th of April 2024). These contributions highlight how strict laws are often the norm in the Chinese context, given the alleged need for higher enforcement efforts for law effectiveness. This relates to the Chinese perspective on the "rule of law," a concept defined by the UN as the "principle of governance in which all entities, public and private, including the State itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated" [22]. The work "How has China formed its conception of the rule of law? A contextual analysis of legal instrumentalism in ROC and PRC law-making" [42] examined the Chinese perception of the rule of law. It concluded that the role played by law in Chinese social governance is limited, which could potentially explain the need for stricter regulations and higher dependency on enforcement for legal effectiveness.

Furthermore, when elaborating on the different goals of data protection regulations in China and Europe, an interviewee shared the following: "*(...) the goal of GDPR is to protect personal data of the individual. So this is to protect the individual. If you look at the [CSL] I think it is not the primary goal. The primary goal (...) is to protect data for the Chinese government*" - (our CMP12 interviewee - 13th of May 2024). This statement points to China's strong collectivist culture[43], which could explain why that is the case. As stated in "Big Data Analytics Sentiment: US-China Reaction to Data Collection by Business and Government", a research paper that examined the perspectives on big data efforts in China and the US, "*China is a highly collectivist culture where people act more according to the interests of the group – and this group may be the government,*" [43]. In addition to that, an interviewee from CMP11 shared the following: "*the point of view of the Europeans in general towards personal data is that of a consumer. So I, as a consumer of services that request data, should have rights. In China, Japan, South Korea, Singapore, and some of the other Southeast Asian nations, data is a personal asset. So long as it provides me convenience, I am willing to share it. People here [Southeast Asia] tend to be more practical or pragmatic in that sense,*" (10th of May 2024). In other words, the perceptions of data alone are subjective to divergent cultural backgrounds. As a result, regulations cannot be analyzed independently from their cultural context.

Culture also plays a role in how different companies internally perceive such regulations. The variations in how regulations are perceived and interpreted because of culture could potentially be a challenge, as highlighted by an interviewee who commented that the "*biggest issue was that my colleagues, who are all Chinese, did not take it very seriously, which is also understandable because again, the way how the law works here is a little bit different. And I had at first to increase the sense of urgency again, not because I believe that we are suddenly the focus of the authorities,*" - (our CMP10 interviewee - 10th of May 2024). Furthermore, two interviewees mentioned how German companies could potentially have an edge over competing external firms in contexts of strict compliance regulations, such as China. According to one of the said interviewees: "*(...) usually German companies have pretty high compliance standards anyway which they apply, and they are coming from the headquarters, and are usually not trying to find a way around or gray areas that they could exploit,*" - our CMP14 interviewee (1st of June 2024). These contributions show that companies operating in China must first understand the Chinese culture as a background for the regulations. Comprehending the social context may act as reassurance of how China operates, diminishing the general uncertainty surrounding the topic. Furthermore, nurturing a strong compliance culture company-wide can be a competitive advantage considering the increasing number of regional data protection regulations coming into effect across the globe [44]. As stated in "EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide": "*Building a corporate culture that believes in the virtue of data protection and in which responsibility and accountability are corporate values will often be the difference between success and failure,*" [45].

6.3 Future Research Topics

6.3.1 Larger Research Sample

An essential step in any research process is to reflect on potential future topics of inquiry that our research could not determine with certainty or new questions generated after analyzing our results. A first potential further step to advance our research topic would be to conduct a similar interviewing process with a larger and more diverse sample group to either confirm our results, providing more evidence that it can be generalized, or reevaluate our conclusions, let that be because of erroneous interpretation or non-representative data. We would highlight the importance of including small enterprises and companies planning to penetrate the market, as their representation was minimal in our research. Besides, our team noticed that companies already active in the market have better access to up-to-date information regarding the regulations. In contrast, outsiders have yet to overcome this barrier when entering the market. Therefore, researching their point of view could yield exciting results on uninformed perspectives on compliance. Besides that, investigating if the loosening of the regulations that occurred in March of 2024 [34] lowered the entry barrier for foreign companies, especially small and medium companies, could also lead to new findings.

6.3.2 Conflicting Perspectives on Compliance Assessment Efforts

Furthermore, we identified multiple conflicting positions in our research results. For instance, while some interviewees mentioned that regulations were becoming stricter, others mentioned they were loosened 5.2.3. Another example regarding enforcement is that some interviewees stated they saw office raids or other invasive types of enforcement practices exaggeratedly depicted, saying that "*Actually, you know, that is always the thing, because there are always a lot of rumors that in China, sometimes it's hard to follow the regulations, so if you do not do it you need to pay huge fines, or you are personally responsible, that you just cannot do it or something like that. That's maybe not wrong, but this happens not too often*," (our CMP13 interviewee - 13th of May 2024). On the other end, other interviewees mentioned frequent audios, for instance: "*local authorities come often to company audits*" (our CMP10 interviewee - 10th of May 2024). The discrepancy intrigued the research team and made us hypothesize about potential explanations behind this phenomenon. Industry segment, company size and data sensitivity could all be possible explanations, however, no convincing correlation involving said variables was identified. A larger empirical dataset could potentially lead to a different outcome. However, after carefully examining the interviewee's responses, we elaborated two possible explanations.

First, given that China delegates significant economic and political responsibilities to lower levels of government [46] and the fact that the regulations are applied by local authorities, such disparity could be explained by different regional enforcement policies or strictness levels. The following contribution supports said idea: *"In Suzhou, for example, it seems that authorities are doing checks, compliance checks on a systematic basis, on a regular basis."* (CMP12 - 13th of May 2024). Furthermore, this hypothesis is supported further by the regional flexibility in the Chinese governmental organization, as discussed in the following statement from the work "Authoritarian Legality in China: Law, Workers, and the State": "*without any constitutional division of powers, the powers that have accrued to lower levels have occurred because of the central government's preference for decentralized governance, greater local autonomy, and competition between regions*" [47].

The second explanation is political pressure. As aforementioned in this research's findings[15], the law triad has allegedly been used politically in the past, so this option cannot be ignored. This perspective is supported by further research on the topic, as in "China's emerging data protection framework": *"They [PIPL and CSL] are the result of years of gradual evolution, influenced by shifts in external factors and the resolution of intellectual debates, but also by political factors including turf battles between different ministries with overlapping jurisdictions and opposition from China's tech giants*," [48].

Further research should examine these cases individually and identify possible reasons to disprove political application. If no political reason can be found and enforcement cases are shown to be random or without proper reasoning, the possibility of power abuse by enforcing authorities may also need to be investigated.

7 Conclusion

This research aimed to tackle how foreign companies in China were affected by the data protection law triad formed by the PIPL, DSL, and CSL. The lack of empirical data on the topic motivated us to approach this question via interviews with companies of various sizes and industries, which we sourced via convenience sampling. The number of interviews conducted was rather small, so our results cannot be generalized to the entire population without additional research. Increasing the sample size could certainly yield additional findings in future research. However, the sourced companies were sufficiently diverse to spark a discussion and elaborate potential answers to this exciting topic.

The interviews painted a picture of general uncertainty towards the regulations. Our results show that the most affected companies are: B2Cs, companies that provide services requiring low latency from servers, businesses located at the end of the supply chain, larger companies storing great amounts of data (above one hundred thousand), and enterprises that are part of sensitive industries defined by the laws. Although a threshold exempting smaller companies from certain requirements was added, SMEs are still strongly affected because of regulatory complexity and the high costs involved in interpreting and assessing if requirements are met. However, if the current flexibilization tendencies and clarification efforts by the government prove to be true, this would allow for compliance ease and an easier self-assessment. In that case, the circumstances for SMEs might become more favorable.

The regulations brought multiple changes for companies, especially regarding acquiring specialized workforce, whether via training, hiring, or outsourcing. Further changes could be seen in regard to strategic adaptations, increased flexibility for local branches, and technology adaptations. While the increase in data protection standards and individual data protection is vastly recognized by industry members as an advantage, legal, financial, and operational consequences were also identified, among which sensitive information leakage, IP and employee protection, compliance costs, and the adaptation of global processes and tools, were mostly mentioned. Furthermore, vague requirements, cross-border data transfers, and complexity were the challenges and disadvantages that were most significantly cited by the interviewed subjects in this research. Our results show a curious conflict of opinions towards the regulations, which we believe is mainly explained by the different familiarity levels with the laws. In this complex scenario, knowledge and strategic planning were identified as the greatest allies of foreign companies operating in the Chinese market.

The collected data led us to believe that, to some extent, the regulations' punishing character or the frequency with which said penalties are imposed could have been exaggerated in the

literature2. Harsh penalties, invasive and aggressive enforcement practices are extensively mentioned in the literature by consulting firms or similar service providers. However, the divergent experiences shared in our research lead us to believe that such cases are not so common in practice or at least not as common as literature implies. We collected a vast range of opinions, with some interviewees mentioning hearing of such extreme cases or even being targeted themselves. Given that regional authorities determined that enforcement, we identified differences in regional control policies as a possible explanation for such different experiences. Nevertheless, individually analyzing cases where companies were penalized and considering the regulations' potential political intent in future research could spark new insights into this discussion. Furthermore, investigating how the recent efforts by the authorities in March of 2024 to loosen regulations will affect the results found in this research is also a prospective research topic, especially regarding SMEs. Therefore, we highlight the need for astute consideration of materials that depict China as a compliance minefield.

Considering the cultural context in which regulatory standards come into effect is particularly important to avoid hysteria and decrease uncertainty. Furthermore, the laws' intentions need to be contextualized because they are China's attempt, as a global power and collectivist State, to tackle the challenge multiple governments face in regulating and protecting national cyberspace. Our results also exhibit the call from foreign companies in China for clarity over vague requirements and definitions but also attest to the government's attempt to compromise regarding the law flexibilizations in March of 2024.

As the interplay between culture, governmental authorities, and companies continues to shape data protection regulations, only future research can further confirm our propositions and identify additional effects of these laws on foreign companies.

8 Appendix

This appendix consists of additional information collected or produced during this research.

8.1 Email Template

Subject: Interviews on Data Protection Law Changes in China with the Technical University of Munich

Dear [Contact Person],

I hope this email finds you well. I am writing to invite you to participate in an interview that the Cyber Trust department of the Technical University of Munich is conducting as part of a thesis research on how companies have been affected by the relatively recent Chinese laws regarding data protection.

Furthermore, I would like to inform you that expertise in the subject is not a prerequisite for participation. The objective of our research is to understand the level of compliance with these regulations within the market. If you're not well-versed in these laws, this could be an opportunity to familiarize yourself with the topic, as we will gladly provide you with an overview.

Your perspective as an industry member, independent of your familiarity with the regulations, is highly valuable to our study. We are eager to gain a comprehensive understanding of how these legal changes have impacted various organizations, and your insights will play a crucial role in achieving this goal. Also, feel free to forward this email to any colleagues or departments that might be interested in this area. I would greatly appreciate it!

This research is being done purely for academic purposes. If you're willing to participate, you will receive a copy of the final results.

Interview Details

- **Date:** a time of your convenience, preferably in May or June
- **Location:** Online via Zoom, Microsoft Meet, or other desired alternatives
- **Duration:** The interview is expected to last approximately 15-30 minutes

- **Language:** The interview can be conducted in either German or English, depending on your preference

– Alternatively –

If circumstances prevent your direct involvement or availability, but you remain inclined to assist our research efforts, would you consider responding to a brief questionnaire? This would significantly contribute to our work. Please respond to this email, and we will promptly send you the questionnaire.

We want to emphasize that your participation is entirely voluntary, and you are not obligated to answer any questions during the interview. Your comfort and autonomy are of utmost importance to us, and we aim to create an open and collaborative environment that encourages candid discussions. Based on your preference, the interview can even be done completely anonymously.

If you are willing to participate, please let us know your availability for the interviews, and we will do our best to accommodate your schedule. If you have any specific expectations or concerns related to the interview, feel free to discuss them with us so that we can ensure a positive and productive experience.

Your input will contribute significantly to the advancement of knowledge in the field of data protection, and we genuinely appreciate your willingness to be a part of this research.

Our interview will primarily focus on the examination of the impact of specifically the Personal Information Protection Law (PIPL), Data Security Law (DSL), and Cybersecurity Law (CSL).

To confirm your participation or discuss any details further, please reply to this email or contact us at [Phone Number].

Thank you for considering this invitation, and we look forward to the opportunity to speak with you.

Best regards,

[Researcher Name]

8.2 Short Email Template

Dear [Contact Name],

I hope this email finds you well. The Cyber Trust department at the Technical University of Munich is conducting interviews for a thesis research project on the impact of recent Chinese data protection laws on companies.

We would like to invite you to participate in these interviews, regardless of your expertise in the subject. Your perspective as an industry member is valuable to our study, and we are keen to understand how these legal changes have affected various organizations.

Interview Details:

- **Date:** Your convenience, preferably in April or May
- **Location:** Online via Zoom, Microsoft Meet, or your preferred platform
- **Duration:** 15 - 30 minutes
- **Language:** English or German, based on your preference

Alternatively, if direct involvement isn't possible, would you consider responding to a brief questionnaire?

Your participation is voluntary, and we respect your autonomy. The interview can even be conducted anonymously if you prefer.

To confirm your participation or discuss further details, please reply to this email or contact us at [Phone Number].

Thank you for considering this invitation. We look forward to speaking with you.

Best regards,

[Researcher Name]

8.3 Git Hub Repository

The following Git Hub Repository includes:

- Coding Results
- Interviewed Companies Overview

https://github.com/TheTrueVester/Analyzing-the-Influence-of-Chinese-Data-Protection-Regulations

8.4 Interviewed Companies Overview

Company	Size	Status	Perception	Familiarity	Industry
CMP01	Small	Advanced	Positive	High	Law Firm
CMP02	Medium	Introductory	Other	Low	Eng./Mfg.
CMP03	Large	Advanced	Positive	High	Consulting
CMP04	Large	Advanced	Negative	Medium	Healthcare
CMP05	Small	Advanced	Other	Low	Eng./Mfg.

CMP06	Small	Advanced	Neutral	High	Consulting
CMP07	Large	Advanced	Neutral	Medium	Insurance
CMP08	Large	Advanced	Neutral	Medium	Eng./Mfg.
CMP09	Large	Advanced	Neutral	Medium	Eng./Mfg.
CMP10	Large	Advanced	Neutral	High	Eng./Mfg.
CMP11	Large	Advanced	Neutral	High	Consulting
CMP12	Medium	Advanced	Positive	High	Law Firm
CMP13	Small	Advanced	Neutral	High	Law Firm
CMP15	Large	Advanced	Neutral	High	IT
CMP16	Large	Advanced	Positive	Medium	Public Trade Assoc.
CMP17	Large	Advanced	Neutral	Medium	Eng./Mfg.
CMP18	Large	Advanced	Neutral	High	Eng./Mfg.
CMP19	Large	Advanced	Positive	High	Eng./Mfg.
CMP20	Large	Advanced	Other	Low	Eng./Mfg.
CMP21	Large	Advanced	Positive	High	Consulting
CMP22	Medium	Intermediate	Neutral	High	Education
CMP23	Large	Advanced	Other	Low	Eng./Mfg.
CMP24	Null	Null	Neutral	Null	Null
CMP25	Null	Intermediate	Neutral	Null	Null

List of Figures

List of Tables

Bibliography

[1] W. M. Morrison. *China's Economic Rise: History, Trends, Challenges, and Implications for the United States*. Accessed: 14.12.2023. 2019. URL: https://www.everycrsreport.com/reports/RL33534.html#_Toc12530866.

[2] *GDP (current US) - China, United States*. Accessed: 10.01.2024. 2024. URL: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=CN-US.

[3] *World Economic Outlook Database: October 2023*. Accessed: 14.12.2023. 2023. URL: https://www.imf.org/en/Publications/WEO/weo-database/2023/October/weo-report?c=924,111,&s=NGDP_RPCH,NGDPD,PPPGDP,NGDPDPC,PPPPC,&sy=2023&ey=2028&ssm=0&scsm=0&scc=0&ssd=1&ssc=0&sic=0&sort=country&ds=.&br=1.

[4] R. Shen and F. Xiao. "Analysis of the Highlights of the Personal Information Protection Law". In: *Deloitte* (2021). Accessed: 10.01.2024. URL: https://www2.deloitte.com/cn/en/pages/risk/articles/personal-information-protection-law-analysis.html.

[5] Y. Lau. *Respect individuals' rights*. Accessed: 29.01.2024. URL: https://edpb.europa.eu/sme-data-protection-guide/respect-individuals-rights_en#toc-7.

[6] *Consent Note for Personal Information Processing*. Accessed: 07.01.2024. URL: https://globalcenters.columbia.edu/content/consent-note-personal-information-processing.

[7] J. Zhu. *The Personal Information Protection Law: China's Version of the GDPR?* Accessed: 07.01.2024. 2022. URL: https://www.jtl.columbia.edu/bulletin-blog/the-personal-information-protection-law-chinas-version-of-the-gdpr.

[8] A. C. Das. *China's New Personal Information Protection Law*. Accessed: 07.01.2024. 2021. URL: https://www.natlawreview.com/article/china-s-new-personal-information-protection-law.

[9] R. Creemers and G. Webster. *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*. Accessed: 02.02.2024. 2021. URL: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

[10] *A comparison of cybersecurity regulations: China*. Accessed: 14.12.2023. URL: https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/china.html.

[11] Y. Lau. *Here's What Beijing's Sweeping New Data Rules Will Mean for Companies*. Accessed: 01.07.2024. 2021. URL: https://fortune.com/2021/09/01/china-data-security-law-beijing-management-regulation-internet/.

[12] S. Sacks and M. K. Li. *How Chinese Cybersecurity Standards Impact Doing Business in China*. Accessed: 19.01.2024. 2023. URL: https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china.

[13] S. Sacks and M. K. Li. *How Chinese Cybersecurity Standards Impact Doing Business in China*. Accessed: 19.01.2024. 2023. URL: https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china.

[14] M. Haldane. *What China's new data laws are and their impact on Big Tech*. Accessed: 2024-2-2. 2021. URL: https://www.scmp.com/tech/policy/article/3147040/what-chinas-new-data-laws-are-and-their-impact-big-tech.

[15] *Didi Chuxing*. Accessed: 07.02.2024. 2023. URL: https://web.didiglobal.com/.

[16] *How the Data Security Law Sets the Stage for the Tech Industry in China and Beyond*. Accessed: 01.07.2024. 2023. URL: https://www.csis.org/blogs/strategic-technologies-blog/how-data-security-law-sets-stage-tech-industry-china-and-beyond.

[17] *China's Data Security Laws Rattle Western Business Executives*. Accessed: 05.03.2024. 2023. URL: https://www.economist.com/business/2023/05/04/chinas-data-security-laws-rattle-western-business-executives.

[18] C. Chen and L. Zhao. "How China's Data Privacy and Security Rules Could Impact Your Business". In: *E. Young* (2023). Accessed: 01.07.2024. URL: https://www.ey.com/en_gl/insights/forensic-integrity-services/how-chinas-data-privacy-and-security-rules-could-impact-your-business.

[19] *10 ways China's new data rules will change your business*. Accessed: 01.07.2024. 2023. URL: https://www.pwc.com/us/en/tech-effect/cybersecurity/china-pipl-rules-impact.html.

[20] *China draft Personal Information Protection Law (PIPL) General introduction and impact analysis*. Accessed: 01.12.2023. 2021. URL: %7Bhttps://www2.deloitte.com/content/dam/Deloitte/cn/Documents/risk/deloitte-cn-ra-personal-information-protection-law-brochure-en-210706.pdf%7D.

[21] P. M. of Industry and I. Technology. *"14th Five-Year" Plan for the Development of the Big Data Industry*. 2022. URL: https://cset.georgetown.edu/publication/14th-five-year-plan-for-the-development-of-the-big-data-industry/.

[22] *What is the Rule of Law*. Accessed: 2024-7-8. URL: https://www.un.org/ruleoflaw/what-is-the-rule-of-law/%20What%20is%20the%20Rule%20of%20Law.

[23] R. Creemers, G. Webster, and P. Triolo. *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*. Accessed: 02.02.2024. 2017. URL: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

[24] DigiChina. *Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)*. Accessed: 02.02.2024. 2021. URL: https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/.

[25] J. Golzar and O. Tajik. *Convenience Sampling*. Accessed: 01.07.2024. 2022. URL: https://www.researchgate.net/publication/366390016_Convenience_Sampling.

[26] D. Skowronek and L. Duerr. *The convenience of nonprobability: Survey strategies for small academic libraries*. Accessed: 01.07.2024. 2009. URL: https://www.researchgate.net/publication/317920223_The_convenience_of_nonprobability_Survey_strategies_for_small_academic_libraries.

[27] AHK. Accessed: 01.01.2023. URL: https://china.ahk.de/market-info/german-company-directory/access/list?tx_cpsfmp_companymainplugin%5Bswords%5D=&tx_cpsfmp_companymainplugin%5Bindustries%5D=0&tx_cpsfmp_companymainplugin%5Bcountries%5D=57&tx_cpsfmp_companymainplugin%5Bregions%5D=0&tx_cpsfmp_companymainplugin%5Bzips%5D=&tx_cpsfmp_companymainplugin%5Bcities%5D=&tx_cpsfmp_companymainplugin%5Bcategories%5D=0&tx_cpsfmp_companymainplugin%5Bahkmember%5D=&tx_cpsfmp_companymainplugin%5Boffers%5D=&submit=.

[28] H. Hsieh and S. E. Shannon. "Three approaches to qualitative content analysis". en. In: *Qual. Health Res.* 15.9 (Nov. 2005), pp. 1277–1288.

[29] *Financing SMEs and Entrepreneurs 2022: An OECD Scoreboard*. Accessed: 01.07.2024. 2022. URL: https://doi.org/10.1787/e9073a0f-en.

[30] *Data protection in the EU*. Accessed: 01.07.2024. URL: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en#:~:text=The%20General%20Data%20Protection%20Regulation%20(GDPR),-Regulation%20(EU)%202016&text=A%20single%20law%20will%20also,applies%20since%2025%20May%202018.

[31] O. for Economic Co-operation and Development. *Enterprises by business size*. 2017. URL: https://www.oecd.org/en/data/indicators/enterprises-by-business-size.html.

[32] A. Acharya and al. "Sampling: Why and How of it?" In: *ResearchGate* (2013).

[33] R. Connolly. *Apple set to build first China-based data centre as regulations harshen*. Accessed: 2024-7-1. URL: https://www.theneweconomy.com/technology/apple-set-to-build-first-china-based-data-centre-as-regulations-harshen.

[34] L. Yu. *A new Regulation facilitates cross-border data transfers from China to a third country*. Accessed: 2024-7-1. URL: https://www.datenschutz-notizen.de/a-new-regulation-facilitates-cross-border-data-transfers-from-china-to-a-third-country-0947297/.

[35] *China's PIPL and DSL*. Accessed: 15.07.2024. URL: https://www.dataguidance.com/advisories/chinas-pipl-and-dsl#:~:text=the%20PIPL%20specifically%20targets%20internet%20platform%20services.

[36] *CHINA AUTO INDUSTRY DATA SECURITY*. Accessed= 15.07.2024. URL: https://www.trade.gov/market-intelligence/china-auto-industry-data-security#:~:text=China%20released%20the%20%E2%80%9CAuto%20data,more%20%E2%80%9Cintelligent%20and%20smart%E2%80%9D..

[37] *China's PIPL and DSL*. Accessed: 15.07.2025. URL: https://www.dataguidance.com/advisories/chinas-pipl-and-dsl#:~:text=Examples%20given%20under%20the%20Standards%20include%20e.g.%20geographic%20data%2C%20biometric%20data%2C%20financial%20data%2C%20military%20data%2C%20and%20data%20of%20sensitive%

20industries%20like%20utility%2C%20transportation%2C%20and%20nuclear%20industries.

[38] D. L. Yu. *A New Regulation Facilitates Cross-Border Data Transfers from China to a Third Country*. Accessed: 25.06.2024. 2023. URL: https://www.datenschutz-notizen.de/a-new-regulation-facilitates-cross-border-data-transfers-from-china-to-a-third-country-0947297/#:~:text=China's%20cross%2Dborder%20data%20transfer,business%20in%20China%20and%20abroad.

[39] *Commission Recommendation of 6 May 2003 Concerning the Definition of Micro, Small and Medium-Sized Enterprises (Text with EEA Relevance) (Notified Under Document Number C(2003) 1422)*. Accessed: 01.07.2024. 2003. URL: http://data.europa.eu/eli/reco/2003/361/oj.

[40] H. Xu and B. Lee. *China Finalises Exemptions to Cross-Border Data Transfer Rules and Eases Restrictions*. Accessed: 15.07.2024. 2024. URL: https://www.lw.com/admin/upload/SiteAttachments/china-finalises-exemptions-to-cross-border-data-transfer-rules-and-eases-restrictions.pdf.

[41] "German Chamber Flash Survey: Price Pressure Amidst Weak Demand Leading Concern of German Companies in China". In: *AHK, German Chamber of Commerce in China* (2024). URL: https://china.ahk.de/publications/flash-surveys.

[42] Q. Wu. "How has China formed its conception of the rule of law? A contextual analysis of legal instrumentalism in ROC and PRC law-making". In: *International Journal of Law in Context* (2017). Accessed: 2024-7-8. URL: https://www.cambridge.org/core/journals/international-journal-of-law-in-context/article/how-has-china-formed-its-conception-of-the-rule-of-law-a-contextual-analysis-of-legal-instrumentalism-in-roc-and-prc-lawmaking/A64927C5B7C8591B914120862DB7694B.

[43] R. C. LaBrie, G. H. Steinke, X. Li, and J. A. Cazier. *Big data analytics sentiment: US-China reaction to data collection by business and government*. 2018. URL: https://doi.org/10.1016/j.techfore.2017.06.029.

[44] *Data Protection and Privacy Legislation Worldwide*. Accessed: 2024-7-8. URL: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[45] I. G. P. TEAM. *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*. IT Governance Publishing, 2020. URL: https://www.jstor.org/stable/j.ctt1trkk7x.

[46] G. Montinola, Y. Qian, and B. R. Weingast. "Federalism, Chinese Style: The Political Basis for Economic Success in China". In: *World Politics* (2011). Accessed: 2024-7-8. URL: https://www.cambridge.org/core/journals/world-politics/article/federalism-chinese-style-the-political-basis-for-economic-success-in-china/6F839D520DAE1BCB2721B36BA5E34396.

[47] M. E. Gallagher. *Authoritarian Legality in China: Law, Workers, and the State*. Accessed: 2024-7-8. Cambridge University Press, 2017. URL: https://books.google.com.br/books?id=b40wDwAAQBAJ%5C&dq=why+aren%5C%27t+laws+in+china+gradual%5C&lr=%5C&source=gbs%5C_navlinks%5C_s.

[48] G. Montinola, Y. Qian, and B. R. Weingast. "China's emerging data protection framework". In: *Journal of Cybersecurity* (2022). Accessed: 2024-7-8. URL: https://academic.oup.com/cybersecurity/article/8/1/tyac011/6674794.