Legal Data Protection Framework Comparison of the United States, European Union, and the People's Republic of China

Karl Asger Juhl
IE University
May 2022

Table of Contents

Executive Summary

Through the rapid advancements and adoption of technologies such as the Internet of Things and AI/ML, the world is moving toward increasingly vast digital economies. This direction can be seen with the growth of big data early-adopters - where the top five big tech companies make up a combined value greater than the next ~25 most valuable US companies together (Ovide, 2021). With a clear trend toward growing digital economies, governments are concerned with the cultivation of a productive digital environment and fostering innovation with hopes of developing the next big tech company. The complex set of objectives countries hold in developing the legal frameworks for data protection range from the long-term success of their digital economy, to safeguarding the rights of their citizens, as well as protecting core services. Regions that implement lacklustre regulations will allow greater exploitation of their citizens, potential attacks on their national security, and a sub-par digital market for both vendors and consumers. The data protection landscapes of the US, EU, and China help illustrate the future's outlook as nations globally follow suit with similar legal approaches to data privacy and security. As with recent movements supporting the protection of individuals' rights and freedoms, much of the provided resources for data protection laws address the rights and protection of consumers. Small and medium sized businesses, as well as entrepreneurs considering launching a data-driven business, must now consider the dimension of data protection laws when considering the expansion or launch of a new business. Serving as a resource for businesses and others seeking understanding of the steps of compliance required, this paper reviews the extent of each country's data protection laws and compares the main components relevant to data-driven businesses.

Literature Review

Data Protection and Cybersecurity in the Digital Age

The wave of the fourth industrial revolution has brought the rapid adoption of technologies such as Artificial Intelligence / Machine Learning (AI/ML), the Internet of Things (IoT), and increasingly superior wireless connectivity. These technologies' common impact is a growth in the production, processing, and accumulation of data globally, as businesses' leverage customer data to optimise the customer experience. The security of the new technologies and their accompanying data has become increasingly important, and has subsequently led to comprehensive data protection frameworks being developed by nations & governing bodies worldwide. The following review of literature substantiates the importance of protecting individuals' personal data, discusses the distinctive regulatory approaches by regions leading AI, and confirms the need for businesses to take actions of compliance for their data activities.

The Need for Superior Data Protection

As consumers use digital platforms, they should be fully informed of how their data is used. This was not the case with Facebook's large scale data breach scandal, which was exposed in 2018, (Meredith, 2018). Meredith gives an encompassing account of the context that made the data breach possible, citing Facebook's actions in opening user data to third-parties. The chronological article spans events from 2010 up until April 2018 when Zuckerberg appeared at Capitol Hill for a joint hearing of the Senate Judiciary and Commerce committees. This breach of user data and its usage by Cambridge Analytica in elections globally make up one of the largest data scandals of the decade, and serves as an important example to look back on and learn from.

With personal data being the key to powering effective AI systems, the protection of such data should be at the forefront of priorities. Cohen, (2020) explored a case study on remote

biometric identity verification powered by AI, with a focus on the personal identifiable information required to make it work. Modern machine learning and AI systems are being scaled up and are fed increasingly large volumes of data, often times personal data. Cohen asserts that as this personal data is the foundation of the effectiveness of modern algorithms, ethical usage of said data should be researched further. The author does so by examining the technical requirements of building AI and how it relates to existing data protection frameworks. The publication proposes that privacy preserving methods should be kept at the forefront of priorities when developing AI systems. The paper provides a perspective on ethics of modern algorithms and the data that they use, and highlights the importance of the protection of personal data in these systems. The ethical considerations of AI usage is becoming more relevant & noticed globally today. Bird, (2021) reviewed China's first set of guidelines on AI ethics, released by the National Information Security Standardisation Technical Committee of China (TC260). The author details important pieces of the guidelines such as a list of actionable recommendations from TC260. Although the guidelines are not released as mandatory requirements for data processors, they are labelled as a national standard. The assertion of non-mandatory standards for the application of AI ethics across industries is a progressive step for the country.

These technologies, such as IoT, cloud-computing, and the usage of AI, are new and larger frontiers for vulnerabilities to be exploited, leaving masses of data points on individuals exposed. The National Academy of Engineering (2019) summarised the proceedings of a forum in 2019 where the focus was on security regulations and other mitigations against cybersecurity attacks. Understanding privacy in new digital contexts as well as building security into AI systems are themes of the discussions. The report includes security discussions around the cloud, the Internet of Things (IoT), and online privacy. Also included in the proceedings are the role of regulators in today's world of complex privacy and security

online, as well as paths forward towards progress in the regulatory space. This report will serve as a reference point for the state of online privacy and security in relation to cybersecurity, AI, and IoT.

The increasingly recognized value of data is one factor motivating a substantial increase in cyber-attacks globally. The Center for Strategic & International Studies (2022) presents a list of all significant cybersecurity incidents ranging from 2006 to present day. The list comprises cyber-attacks on government agencies, defence and high tech companies, as well as economic crimes which caused losses of more than one million dollars. The nature of the cyber-attacks are widely varied, from Russian interference with Ukrainian cyber infrastructure in the Russian invasion of Ukraine, to China accusing the NSA of engineering backdoors. This verified list is a highly valuable resource for this paper and it aids in justifying the need of superior cybersecurity systems to prevent attacks.

Large scale infrastructures are more often being targeted by hackers, as these systems can often be critical to a country's economy & needs. Das, (2019) conducts an analysis on modern cyber-attacks with respect to major critical infrastructure sectors. The paper explores the most common tactics used in cyber-attacks on critical infrastructure, giving an overview of recent cyber-attacks and their characteristics. The author supplies important information while presenting and explaining cyber-attacks on critical infrastructure which have taken place in recent years.

The United States has legislated data protection frameworks, but mostly on a state-level basis, rather than enacting a federal-level data protection framework. The congressional research service (CRS, 2019) provides an in-depth review of the range of data protection statutes and legislation in place in the US. Information includes comparisons to the EU's GDPR and explains contrasting differences. The report was compiled in order to inform Congress on the topic in the case that Congress considers developing a comprehensive federal data protection

law. The report cites inadequate cybersecurity practices which have led to the exposure of millions of Americans' electronic and personal data. The overview asserts that the current legislations on the topic lack uniformity at a federal level, and only regulate certain industries and subcategories of data. This report goes into detail on each major data protection legislation in place in 2019 and thereby gives an overview of American data protection policies.

Progress in Data Protection

California's Consumer Privacy Act (CCPA) is viewed as the most progressive data privacy framework currently enacted in the US. California's Department of Justice's website (OAG, 2019) includes a webpage that includes all-encompassing information of California's CCPA. Upon its enactment, Bahar (2018) provided a brief overview of California's CCPA in June of 2018. The law firm authoring the report offers a summary of the CCPA rules, and makes comparisons between it and the EU's GDPR. The report gives an explanation of differences between the CCPA and GDPR and the information proves useful for the comparative purpose of this paper. In addition to these sources, the office of the attorney general of California's Department of Justice (OAG, 2019) provided a fact sheet regarding the CCPA. This document includes the applications and implications of the CCPA and offers ease of understanding the purposes of the new state legislation.

The CCPA took inspiration from the EU's GDPR, and Jehl, (2018) developed a practical comparison between the EU's GDPR enacted in May of 2018 and California's CCPA. The comparative report is built in a table format which directly compares the technical and legal differences between the two data protection frameworks. Information compared across categories includes who is regulated and protected, as well as what types of information are protected, what security measures are required for data processors, and more. The report gives

an important overview of the two legislations, which will aid the required research in comparatively analysing the data frameworks of the EU and US.

As the US has not developed a comprehensive data protection framework covering all states, California's privacy act is not the final solution for the country. Klosowski, (2021) explains the current state of data protection laws in the US to the public audience of the New York Times. Referencing various breaches of consumer data, the author makes the point that consumer data privacy laws need to be implemented more effectively in order to serve their purpose. By collecting various perspectives of legal professionals, the article gives an overview of the issues with current data protection legislation in the US. Recommendations are made on the basis of privacy experts, pointing to key areas that citizens deserve basic rights in, such as data collection and consent. This article builds important arguments for the improvement of data protection laws in the US.

The leading nations of the world are competing to be leaders of AI systems, which makes any legislation regarding the data required for such systems a globally political issue. Walters, (2021) published a practical guide & comparison of data protection laws of China, United States, and other countries. Authors Walters and Novak explore the intersection of AI, cyber security, and data protection in these nations. The authors make recommendations towards regulators in governments to launch research and legislative reform with a wider scope. The book highlights the importance of ensuring the protection of personal data for all, while balancing the benefits of the digital economy. The vast comparisons of cybersecurity and data protection legislation across regions provides further perspectives on global data protection matters.

Diverging Regulatory Strategies

The topic of AI and national data strategy can be considered from the highest level as global flows of data. Burri, (2021) explores the transformation of the value of data in today's world.

The publication examines global data flows, evaluating strategies such as data protectionism. The ideas of global flows of data are then analysed from the perspective of today's applications of big data and AI. The new relationships between law and rights of online users are explored, with focus on user privacy. Several different regional perspectives on the regulation of data are explained - from China, Latin America, Canada, and Europe. This publication informs on the latest findings in global data flows, privacy, and their respective regulation.

With strategies such as data protectionism, it is important to examine a nation's policies together in order to evaluate the nation's strategy and potential goals. Graham, (2021) examines China's Personal Information Protection Law (PIPL) and its evolution from the first draft in 2020 to its completion in 2021. Graham investigates significant amendments in topics such as automated decision-making and data portability. The paper also analyses how the PIPL fits in with China's set of 'near-complete' cyber-security laws. The author builds an argument that the PIPL and its set of data export conditions are more than just asserting data protection rights for the citizens of China, as it also helps the nation strategically negotiate 'mutual data export agreements'. Such strategic positioning would support progress in AI and the digital economy. Grotto, (2019) examines China's aims to be a leading centre for AI and digital innovation by 2030. Through multiple experts and translators, various perspectives are shared regarding China's aspirations towards AI, the strategy behind it, as well as the political and ethical aspects of the topic. The critical expert evaluations of China's strategy and AI development provide valuable insights on the topic.

Data Protection

The US, EU, and China have taken different paths in the manner they build data protection regulations. Boyne, (2018) contrasts the US regulatory approach with Europe's Data Protection Directive which was in place before the General Data Protection Regulation

(GDPR). The report also gives information on the complete evolution of personal data protection in the US since 1970. As explained in the report, the US uses a sectoral approach to regulating data privacy, and the report gives an overview of regulation in each of these areas. Harmonising IT laws between nations would be the optimal approach to allow for a fully connected digital world, with fewer barriers. Kontargyris, (2018) makes recommendations on paths forward for global IT laws of the future based on the findings of research in the information and communication technology (ICT) field. The book examines the current legislations of the US and EU comparatively, specifically with regard to data privacy and protection. The author explores the rationales of different schools of thought and respective legal structures of data legislations.

Minor differences in legislating data protection can have a large impact on businesses seeking compliance. Lynn, (2021) provides a comprehensive overview of cloud computing and big data from a legal perspective. The third chapter of the book delves into the challenges of regulating borderless cloud computing as well as the differences between US and EU data privacy laws. The author explains the wide range of privacy related matters which can accompany cloud computing. The practical application of ethical theory in cloud computing is discussed, including points on data ownership and data privacy. Key chapters in this publication provide insight to best practices and latest findings in the field, as well as useful comparisons across regional approaches.

Cybersecurity

Cybersecurity activity between countries is not shown in the news each day, but it is complex and constantly evolving with the basis of international relations. Lewis, (2021) builds an argument that American cyber strategy is not sufficient and relies on obsolete ideas and objectives. Pointing to the bigger picture of relations with China and Russia, Lewis asserts that cyber strategy should be embedded in the relating policies and strategies of these

international relations. The US, the author argues, should increase its cyber capabilities both technically and in unity with allies in terms of communication and coordination. The report discusses the cyber relations between China and the US, suggesting that the American government take more assertive actions in the cyber space in order to improve its position in negotiating a relatively less dangerous cyber-space. The report gives important contextual information in the cyber relations between China and the US, and makes several recommendations for the US to advance its position in cyberspace.

As cybersecurity policies can be used to interpret a nation's position in international cyber-relations, they must cover all facets of markets. Banasiński, (2021) explores the growing issue of the cybersecurity of consumer products within the European market. The author cites the growth of smart products and the IoT market as accelerators for the problematic cybersecurity of products intended for consumers. The publication examines the EU cybersecurity model and the current state of implementation of said model, and the role of consumer protection authorities. The report also identifies the steps needed for synthesising legislation between EU cybersecurity regulations and consumer product safety laws.

The EU was one of the first leading governing bodies to enact a comprehensive data protection framework, and has served as an example globally. The European Data Protection Supervisor (EDPR, 2018) website hosts a web page dedicated to the history of the GDPR. Information is given on many steps of the evolution including the initial discussions and opinions of the European Commission to build and adopt a comprehensive approach to personal data protection. Despite the seemingly all-encompassing nature of the GDPR, some aspects of policies are left ambiguous. Papakonstantinou, (2021) analytically reviews the EU's state of cybersecurity from a policy standpoint. The publication points out the lack of clarity of the meaning of cybersecurity within the EU, specifically whether it is meant as a praxis or as a state. The author also explores the path forward and examines the possibility of

the EU amending an additional right to cybersecurity for its member-state citizens. This report gives a perspective on the cybersecurity policies of the EU and sheds light to how the future may look.

Data Processing

Differences in data handling & processing requirements between regions presents a challenge for global businesses seeking compliance while optimising their digital operations. Brumfield, (2021) explains the objectives, conditions, and interpreted priorities of China's Personal Information Protection Law (PIPL). Brumfield points out inherent differences in the Chinese regulation of data protection compared to Western frameworks. He also goes on to explain the nature of these frameworks, which had yet to give specific guidelines on how global companies operating in China could work to comply with the new laws. The text gives insightful perspective on the new legal frameworks, their objectives, and potential impacts. Mok, (2021) reviews China's Data Security Law (DSL), one of the central laws making up the modern data and cybersecurity legislation framework. Mok highlights the most impactful conditions created in the DSL, as well as the obligations imposed on companies meeting those conditions. The author explains the approach of the legislation and how it applies to different industries.

The divergence in nations' paths of data protection legislation provides understanding of the big picture of cyber-relations today. Chow, (2021) overviews legislative updates from both China and the US in late 2021, specifically reporting on new laws relating to national data protection. The legal review provides insight into how the US and China are both developing their data protection legislation. Pernot-Leplay, (2020) compiled research on the historical developments of China's data privacy laws and compares the strategy with those of the EU and US. Pernot-Leplay finds that while China began on the strategic legal path similar to the US, the recent legislations follow the moves the EU took in developing GDPR. The author

studies each strategy in detail but analyses the Chinese laws most thoroughly, finding the characteristics which make Chinese data protection legislation unique to the other frameworks around the world. This article gives an important overview of all three frameworks and especially offers insight into the unique differences in Chinese data privacy legislation.

One of the largest impacts China's new regulations on data processors will be the changes to proper compliance which companies will have to adhere to. Mok, (2021) provides insight into the changes which businesses may need to make in order to be in compliance with new cybersecurity regulations. The new Chinese framework is dissected by each major law, from new review mechanisms for companies operating with mass user data, to the required security certifications for cyber products in the country.

Seeking Compliance Across Markets

The highly digital world of today requires protection for users' data online, which has been legislated in comprehensive data protection frameworks across the world. This regulatory field is constantly evolving and presents businesses using data with challenges to comply with the different regulations globally. This literature review has provided a short historical and current account of data protection frameworks of the EU, US, and China, however, further research presenting the practical differences for businesses seeking compliance in these regions would be beneficial.

Methodology

This paper aims to serve as a resource to individuals or organisations interested in gaining understanding of the data protection landscapes in the People's Republic of China (PRC), United States (US), and European Union (EU). These environments will be summarised in terms of the current relevant legislation, ranging from the legal definitions of personal data to the range of enforcement actions used in each region. Contrasting aspects between the regions will be highlighted to further inform the reader on the most crucial similarities and differences between the regions. An additional deliverable supplementing the paper will be produced in the form of an infographic built using a visualisation tool. This item will encapsulate some of the most important and contrasting aspects of the data protection landscape across regions. It will allow individuals to quickly and easily understand the high level differences between the US, EU, and PRC's legal data protection environments.

In order to build the summary of each region's legal data protection frameworks, the respective region's official legislation has been used in combination with other resources giving insight and explanation to the official legislation. In the interest of making the summaries more productive for readers, the topics discussed have been standardised across regions.

The deliverable items will contain several quantified dimensions of data protection legislation across regions. Such figures will be explained and make up a graphic which communicates key differences within major areas of data protection compliance. Any data used in producing the infographic is extracted primarily from official legislation.

The European Union's Data Protection Laws

Legislation

The European Union set forth the General Data Protection Regulation (GDPR) in 2016 before coming into effect in May of 2018, following a two-year transition period (Regulation 2016/679, 2016). The regulation is equally applicable in each EU Member State and does not require member states to implement their own national laws, although there are numerous areas allowing more domestic legislation.

Since the implementation of the GDPR, the EU commission continues to move forward proposed bills which further aim to regulate and curate a digital ecosystem within the union. These efforts include the Data Act, the Digital Markets Act (DMA), and the Digital Services Act (DSA), which are each in the final legislative processes between the EU parliament and council. The Data Act seeks a more equal ground level for the world of data in the EU - the access to data will be standardised, giving people stronger rights, as well as improving the access that public sector organisations have on data in the private sector (Data Act 2022/0047, 2022). The DMA and DSA address problematic areas of the increasingly prominent digital platforms of today (Digital Markets Act 2020/842, Data Act 2022/0047, 2020). Citing issues such as manipulative spreading of disinformation and the trading of illicit goods and services, the regulations impose rules on large 'gatekeepers', which aim to set up and maintain a more even playing field on the digital markets which platforms provide access to.

Territorial Scope

In general, the GDPR is applicable to those organisations operating in the EU and conducting data processing activities. The scope also extends to organisations established outside of the EU. This would apply when an organisation processes EU individuals' personal data for the

offering goods or services to EU individuals (even if the cost is free), or when an organisation monitors the behaviour of EU individuals (Article 3 Regulation 2016/679, 2016).

Definitions

The European Union's GDPR adopts the definition of 'personal data' to be 'any information relating to an identified or identifiable natural person' . Unlike US privacy laws, a name is not needed in combination with other identifiable data points - just a phone number linked to a person would be personal data under the GDPR definitions. Online identifying data, such as cookies and IP addresses, are specifically ruled as personal data as well (Article 4 Regulation 2016/679, 2016).

The GDPR classifies some categories of information into 'special categories', including information related to health, biometrics and religious beliefs, upon which the regulation imposes processing restrictions. Processing restrictions are also placed on personal data relating to criminal offence information (Article 9 Regulation 2016/679, 2016).

The GDPR refers to 'processing' as operations executed on some data, whether it be the storing or deletion of data, or more.

The GDPR refers to the 'controller' or 'processor' as the entities permitted to process the personal data of people in the EU. The controller as an entity independently chooses the purposes & means of processing operations on personal data. The processing entity performs processing operations on personal data for the controller as instructed (Article 4 Regulation 2016/679, 2016).

Meaning of the 'data subject' is given to be an individual in the EU whose personal data is processed by a processor or controller.

'Personal data breach' is defined as some security breach which leads to the unlawful or accidental loss, destruction, access to, or disclosure of personal data.

National Data Protection Authority

Enforcing the GDPR in each Member State is the responsibility of the national data protection regulator, or supervisory authority. At the EU level there is the European Data Protection Board which is made up of representatives from each national supervisory authority, and is responsible for monitoring and guiding the consistent enforcement of the regulation.

For cases of data protection enforcement where activities span across Member States, the GDPR establishes the idea of a 'lead' supervisory authority to be the leading authority (Article 56 Regulation 2016/679, 2016). In such cases, the 'lead' authority is the one which governs the region in which the controller's main establishment is located.

Registration

In the European Union there is no law obliging individuals or businesses to register data processing activities with authorities. The GDPR does require communication between controllers and authorities in certain cases, and the contact of the data protection officer of the controller should be given to the supervisory authority.

The GDPR asserts strict requirements for internal accountability of controllers, which often supersedes external accountability to authorities. Controllers and processors' internal accountability requirements include maintaining comprehensive documentation of all processing activities. Such requirements are quite demanding for a large business, especially given that the documentation must be produced to a supervisory authority on demand.

Data Protection Officers

The GDPR sets forth the requirements to appoint a data protection officer (DPO), if a controller meets at least one of the following conditions:

- Its main activities include large-scale sensitive personal data processing

- Its main activities include processing operations of regular or systematic monitoring of individuals on a large scale
- It is a public authority

Through ownership or control in a company, groups of ‘undertakings’ can hire one DPO, as long as the officer remains contactable from all establishments (Article 37 Regulation 2016/679, 2016). While it is permitted to only appoint one data protection officer for a large corporation, it will find difficulty in maintaining all compliance requirements across establishments.

The DPO is legally required to be an expert on data protection law and best practices. Outsourcing the role of the DPO to a third-party service provider is permitted (Article 37 Regulation 2016/679, 2016).

Controllers are obliged to ensure the DPO is duly concerned with processing activities and namely the protection of personal data held by the organisation. The GDPR also states that the DPO should report to top management, and should not be directed away from their primary duties (Article 38 Regulation 2016/679, 2016).

The GDPR specifies the tasks of the DPO role (Article 39 Regulation 2016/679, 2016):

- Give advice on GDPR compliance as well as other relevant laws
- Work with authorities as the point of contact of the organisation
- Propose and oversee DPIAs where applicable
- Monitor compliance, both internally and externally

Data Collection & Processing

Principles

The GDPR set forth a set of core principles by which controllers are responsible for complying across all personal data processing activities (Article 5 Regulation 2016/679, 2016). These principles direct that personal data must be:

- Relevant, adequate, and limited to the necessary data for the given purposes
- Collected for the specific, explicit, and legitimate purposes, and not further processed in a way incompatible with the said purposes
- Lawfully, transparently, and fairly processed
- Accurate and maintained as current where applicable
- Stored in a manner allowing identification of people for a time limited to the purpose
- Processed in an environment secured by use of technical and organisational measures

Controllers must demonstrate and maintain compliance with the core principles. Not only will organisations need to comply in the present day, but also demonstrate compliance in regard to processes and personal data in question from years before. This imposes documentation and auditing as key factors that will help an organisation achieve the accountability required by the GDPR.

Legal Bases for Processing

Under the GDPR, all use-cases for personal data processing activities must be justified with one of the given legal bases (Article 6 Regulation 2016/679, 2016):

- When necessary in complying with legal obligations where the controller is the subject
- When necessary in performing tasks carried out in the interest of the public
- When necessary for protecting the vital interests of the individual or other
- When necessary for legitimate interests of the controller or third-party. (Tested through a balancing test of the interests of the controller versus the rights and freedom or interests of the individual(s))

- When necessary in completing a contract in which the individual is a party – or under the request of the individual before entering a contract
- With consent of the individual, which must include an opt-out choice

Special Category Data

The processing of data classified in the 'special category' is restricted to certain uses (Article 9 Regulation 2016/679, 2016). There are 10 listed exemptions allowing the processing of such data types, ranging from explicit consent of the individuals to public health interests, to human resources activities within a company. These exemptions function as a secondary set of bases mandatory for special category data, which should be referenced in addition to one of the Article 6 bases above.

Member States may introduce additional domestic laws further regulating the processing of special category data.

Criminal Offence Data

Processing personal data related to criminal records is prohibited by the GDPR except when authorised by Member State law or carried out by an official public authority (Article 10 Regulation 2016/679, 2016).

Secondary Purpose

Due to the purpose limitation principle of data processing in the GDPR, the use of personal data must be compatible with the initial purpose stated to the individual. Controllers are able to discern whether new processes' purposes are compatible. The regulation also imposes specific factors that the controller must consider in assessing the secondary purpose of personal data (Article 6 Regulation 2016/679, 2016):

- Links between new and initial purpose
- Context of the data collection

- Whether the data includes any special category or criminal record information
- The potential effects on individuals derived from further processing
- The presence of encryption, pseudonymization, or other safeguards

Given that a controller deems the purpose of the new process to be incompatible with the original purpose - the controller must seek the explicit consent of individuals as the remaining legal basis for processing.

Transparency

The GDPR aims to help individuals understand why their data is used, and what actions they can take in relation to their personal data being processed. In order to build this level of transparency, the GDPR asserts a set of details that the controller must present to the individuals in a clear and transparent manner, using plain language. The content which must be presented to individuals at the time of collection includes the contact information of the DPO and controller, the specified purposes of data collection & the respective legal basis, the future recipients & destinations of the data, the length of retention, as well as stating the relevant rights that individuals hold through the GDPR (Article 13 Regulation 2016/679, 2016).

In cases where data was not collected from the individual, a different set of requirements apply, detailed in Article 14 of the GDPR.

Rights of the Individual

Through the implementation of the GDPR, individuals hold substantial rights to govern their personal data and its processing by businesses. Controllers are required to present data on their actions in response to individuals' requests with respect to their personal data. By default, a controller is given one month to provide such information, although this period may be delayed by another two months in cases of onerous requests.

‘Right of access’: Individuals hold the right to request access & attain a copy of their personal data records, along with information summarising the use of the data by the controller (Article 15 Regulation 2016/679, 2016).

‘Right to rectify’: Individuals hold the right to request inaccuracies and incomplete personal information to be rectified through corrections and completion with up-to-date information (Article 16 Regulation 2016/679, 2016).

‘Right to erasure’: Individuals hold the right to request the deletion of their personal information. This right is not as absolute as the other rights held by individuals – it is applicable in certain circumstances, such as when the controller has already used the data for its specified purpose (Article 17 Regulation 2016/679, 2016).

‘Right to the restriction of processing’: In specified circumstances, individuals hold the right to restrict how their personal data is processed. This can happen when individuals dispute the accuracy of the data, protest the erasure of the data, the controller has already fulfilled its original purpose but can’t yet erase it due to retention obligations, or when the decision of the individual’s objection to processing is pending (Article 18 Regulation 2016/679, 2016).

The ‘restriction’ within this right means that an individual’s personal data, beyond storage, may only be processed given your consent, for legal claims, or for public interest of the EU. This right gives the ability for individuals to ensure that their personal information is not processed for unwanted purposes in the future, in cases where organisations are obligated to store customer information for a minimum period.

‘Right to data portability’: Individuals hold the right to request a copy of all their personal data from a controller, given that the controller has lawfully processed the individual’s personal data through consent or other means (Article 20 Regulation 2016/679, 2016).

‘Right to object’: Individuals hold the right to object to the processing of their data when the controller is using their data; for tasks carried out in the public interest, for their legitimate

interests, for the exercise of official authority, for direct marketing or statistical purposes, or scientific or historical research purposes (Article 21 Regulation 2016/679, 2016).

In the case of an objection, the controller in question must suspend the processing of the individual's personal data until strong and legitimate reasons are given to justify the processing, effectively overriding the individuals' rights.

When direct marketing is the given purpose of the controller, individuals hold the definitive right to object to their personal data's processing at any time.

'Right to inhibit automated decision making': Individuals hold the right to not be subject to a decision based solely on automated processing or profiling, which creates legal impact or somehow significantly affects them (Article 22 Regulation 2016/679, 2016).

Automated decision-making with legal or similarly significant effects, may only be carried out by a controller if the decision is;

- Authorised by EU law
- Necessary for entering or performing a contract between the individual and organisation
- Based on the individual's explicit consent

Significant automated decision-making completed on the basis of the first two purposes contains further requirements which allow the individual to obtain human intervention, express their viewpoint, and obtain explanation of the decision & challenge it.

Data Transfer

The GDPR sets forth obligations by which all data transfers involving personal data and leaving the European Economic Area must meet (Article 44 Regulation 2016/679, 2016). In addition to the conditions allowing data transfers outside of the EEA, the European Commission holds the power to decide whether a given country provides adequate data

protection and can be permitted to openly receive transfers of personal data from EU Member States (Article 45 Regulation 2016/679, 2016). As of April 20, the commission has recognized Canada, Argentina, and Switzerland among the 14 countries granted adequacy decisions.

Data transfers to other countries are still possible when meeting the requirements stated in the GDPR, mainly pertaining to appropriate safeguards in combination with the continued availability of enforceable rights and legal solutions for individuals. The appropriate safeguards stated in the GDPR include the implementation of binding corporate rules, standard contractual clauses ensuring appropriate data protection, and the adherence to a code of conduct as well as the procurement of binding and enforceable commitments from the recipient abroad to apply appropriate safeguards to the data. Part of the obligations set forth in this regard are imposed by the GDPR to ensure that EU persons' rights are protected even when their data is transferred internationally and processed elsewhere.

Aside from the conditions stated above that grant the possibility of data transfer abroad, the GDPR includes a list of additional exemptions which permit the transfer to other countries, when:

- The individuals have given explicit consent after being informed of risks
- The transfer is necessary for the implementation of pre-contractual measures or the completion of a contract amid the controller and individual
- The transfer is necessary for the completion of a contract amid the controller and some person in the interests of the individual
- The transfer is necessary for the establishment, exercise or defence of legal claims
- The transfer is from a database which is regarded as intending to present information to the public, according to EU or Member State law

- The transfer is necessary to protect the vital interests of the individual in cases where consent cannot be solicited
- The transfer is necessary for important reasons of public interest

Furthermore there is a final, narrow exemption which controllers may rely on when no other mechanism suffices and the data transfer is essential for the legitimate and compelling interests of the controller - where the rights of the individual are not suppressed. Using this exemption, the controller must notify the supervisory authority as well as each of the relevant data subjects.

International agreements such as mutual legal aid treaties impose the basis on which data transfers requested by official legal authorities of foreign nations are recognised and permitted (Article 48 Regulation 2016/679, 2016).

Security

The GDPR sets forth a proportionate approach to standard security measures which should be adopted depending on the context of the processing activities. This approach requires that controllers and processors implement an appropriate level of security through both technical and organisational measures, given the level of risk of their processing activities. Controllers and processors must consider factors such as the scope and purposes of their processing activities, as well as the cost of implementation for various security measures.

The regulation does, however, set forth these considerations toward controllers and processors in judging appropriate security:

- Implementation of pseudonymisation, or the encryption of data
- -Measures that restore the availability and access to personal data in the event of a breach or some incident
- Ensuring continued resilience, availability, and confidentiality of processing systems

- Processes that systematically evaluate the effectiveness of security measures

Breach Notification

Controllers must notify supervisory authorities of personal data breaches, and additionally notify affected individuals for more significant breaches.

In the case of any security breach that poses some risk to the rights or freedoms of data subjects, controllers must promptly notify supervisory authorities within 72 hours of becoming aware. In cases where breaches pose significant risk to subjects, the controller must notify affected data subjects. However, if a controller deems a breach to be unlikely in posing any risk to the rights and freedoms of data subjects, they are not required to notify authorities (Article 34 Regulation 2016/679, 2016).

When the processor is responsible for a breach of security, they must notify their controller without delay (Article 33 Regulation 2016/679, 2016).

The regulation sets forth requirements for the content of the notice to supervisory authorities. These required bits of information include: contact information of the DPO, the individuals & data types affected, probable effects of the incident, and any remedial measures taken by the controller.

The GDPR sets a further requirement on controllers to maintain the documentation of each data breach, even those not notified to authorities, and, on demand, allow the auditing of such records by the authorities (Article 33 Regulation 2016/679, 2016). There is no stated length of time for which such documentation should be held, which highlights the importance of effective documentation processes for businesses seeking compliance.

Enforcement

Fines

Supervisory authorities hold the power to enforce GDPR rules through financial penalties with a max ceiling of the greater figure: 4% of annual global revenue, or EUR 20 million.

Each supervisory authority in the Union is vested with the power to impose administrative fines in cases of GDPR violations. Relevant circumstances of each case are considered in determining the level of the fines, including the type, severity and length of the infringement, as well as its respective consequences and the actions taken since. Recital 150 continues to state that in cases where administrative fines are imposed on undertakings, the concept of undertakings should be understood according to the meaning set forth in Article 101(1), (Article 101(1) TFEU, 2009). The interpretation and classification of the subject as an undertaking will be decided on a case by case basis, allowing great legal room for regulators to decide. This can have detrimental effects on large corporations as in past case law, regulators have imposed sanctions onto parent companies for the fines imposed on their subsidiary companies. The impact of this is where a controller is a small subsidiary of a large group company, the group company's revenue would be the reference for the fine, and be responsible for the damages as well.

Where such fines are imposed on individuals not an undertaking, supervisory authorities consider the general level of income in the respective Member State, as well as the economic situation of the individual, when determining the appropriate amount of the fine.

There are two classes of fines for the enforcement of GDPR rules, the lesser, and greater, monetary penalties (Article 83 Regulation 2016/679, 2016).

As mentioned, the ceiling of the greater set of penalties is EUR 20 million or 4% of the global revenue of the previous year, depending on which fine is greater. These fines apply to infringements on:

- The GDPR principles of processing - including consent conditions
- Lawful cross-border transfer of personal data
- Any obligations set forth by Member State law
- Non-compliance with orders or limitations set forth by supervisory authorities
- The rights of the individual

The lesser fines have a ceiling of EUR 10 million or 2% of global revenue, depending on which fine is greater. These fines apply to infringements on the:

- Obligations of the controller & processor
- Obligations of the monitoring body
- Obligations of the certification body

Although the supervisory authorities are not obliged to impose fines in every case of infringement, they must ensure that the sanctions are effective and proportionate to the violations. Sanctions may also be imposed in combination with financial penalties.

As with many areas of the GDPR, EU Member States may tailor the style of enforcement – Spain, for example, has three varying levels of infringements, with respective limitation periods being the associated sanction for the level of infringement.

Investigative Powers

Aside from financial sanctions and limitations, supervisory authorities also hold the power to conduct on-site data protection audits, issue public warnings, reprimands, and orders with the purpose of remediating the situation (Article 58 Regulation 2016/679, 2016).

Individuals' Right to Claim Compensation

The regulation specifically asserts the power for individuals to sue controllers or processors for violating their rights. With this, individuals who have suffered 'material or non-material damage' as a result of GDPR violations, may receive compensation from the liable controller (Article 82 Regulation 2016/679, 2016). Moreover, through the wide definition which includes non-material damage, individuals who are unable to prove financial suffering still hold grounds for compensation.

Individuals hold the right to have a relevant consumer protection agency exercise their rights by filing suit against controllers on their behalf (Article 80 Regulation 2016/679, 2016).

Farther than these specified provisions, individuals hold a right to file complaints with a supervisory authority (Article 77 Regulation 2016/679, 2016). Data subjects also hold the right to efficacious legal remedies against controllers or processors (Article 78 Regulation 2016/679, 2016).

All people, controllers, and processors carry the right to legal remedies against a decision or lack of decision of a supervisory authority (Article 79 Regulation 2016/679, 2016).

E-Marketing

Given the GDPR's wide scope of personal data, most electronic marketing will have to comply with GDPR regulation since it leverages personal data points for each subject for profiling purposes. The most common and plausible legal basis for e-marketing activities is consent, for which the GDPR gives detailed requirements.

EU data subjects always hold the right to object and halt direct marketing activities (Article 21 Regulation 2016/679, 2016).

The EU's ePrivacy Directive from 2002 specifies rules on electronic marketing, which are transposed into Member State laws. The directive's 2009 update resulted in the cookie opt-in mechanisms that popped onto the internet as websites complied with the EU privacy law. This

directive is currently under legislative procedures to be updated with the ePrivacy Regulation, which will be uniformly applied across the EU.

Electronic marketing is an area which is generally regulated more specifically within each Member State's legislation.

Online Privacy

Gatekeeper Regulation

Through the proposed Digital Services Act (DSA), the commission imposes obligations to all online intermediary service providers, proportionate to the nature and size of the platform (Digital Services Act 2020/825, 2020). The regulation exempts smaller platforms with less than 45 million active monthly users, while those with more than the figure are labelled as very large online platforms (VLOP) and are subject to heavier regulation. The DSA seeks to complete a few main objectives:

Empower users and society by:

- Enabling users to challenge content moderation decisions
- Enabling access to platform data for authorised researchers and NGOs
- Imposing transparency measures on the algorithms of large platforms

Reduce risk through:

- Independent auditing of risk management systems
- Mechanisms allowing efficient reaction to public health crises
- Safeguards for minors online & limiting sensitive personal data in targeted ads

Curate a safer environment with:

- Mechanisms enabling users to 'flag' illegal goods, services, or content online
- Obligations of traceability for business users in market places

In addition to these imposed measures, the DSA imposes enhanced supervision of VLOPs by the EU Commission. Furthermore, the DSA establishes digital services coordinators, who, responsible for investigations and enforcement of the DSA, must be appointed in each Member State.

The Data Markets Act (DMA) regulates large, core platform services with the aim of developing a more competitive and level playing field within the EU digital market and globally (Digital Markets Act 2020/842, 2020). The DMA is applicable to 'gatekeepers' - organisations which earn €7.5 billion annually or are valued at €75 billion in combination with maintaining 45 million monthly users as well as 10,000 business users in the EU. The organisation should run core platform services in at least 3 Member States, including social networks, search engines, ad services, voice assistants and web browsers. Small and medium businesses are exempt from DMA regulations, as an effort to foster an environment of innovation.

Those organisations ruled as gatekeepers are obligated to begin specified practices as well as halting previous practices within their platforms. Gatekeepers must provide greater transparency to users as the EU commission, and vendors on marketplaces. The DMA seeks to increase fairness in the digital environment, and therefore gatekeepers must no longer rank their own services higher than competitors, reuse private data for additional purposes, use conditions which are unfair to vendors, pre-install applications, and require platform developers to use specified services in order to be listed on the platform.

Cookies

Through the ePrivacy Directive implemented in each Member State, the use of cookies and comparable tracking devices requires:

- Consent of the website user
- Presentation of clear and comprehensive information

Cookies do not require consent when they are only used in electronically communicating over the internet, or when they are strictly required for completing a service requested by an individual.

The People's Republic of China

Legislation

The People's Republic of China (PRC) does not have one comprehensive data protection law, and instead has a complex framework where rules are present across various laws. Recent years have seen the PRC put in place the three pillars of their personal information protection structure: the Data Security Law (DSL), the Cybersecurity Law (CSL), and the Personal Information Protection Law (PIPL).

The CSL was the first to come into effect by 2017, addressing data privacy and cybersecurity. In 2021, the DSL came into effect, which focused on the security of data across categories, rather than only the security of personal data. The PIPL is the latest and most significant law to come into effect – being the first comprehensive legislation regulating the protection of personal information and data of people in China. The Chinese data protection framework took inspiration from the GDPR throughout various aspects, thus the overall legal structure is similar, though not identical.

Territorial Scope

The scope of the PIPL is extra-territorial, in that it applies to the following activities:

- Data processing in the PRC involving residents' personal data, and

- Data processing of PRC residents' personal data from **outside** of the PRC for:
    - Offering goods or services to individuals in the PRC
    - Evaluating the behaviour of individuals in the PRC
    - Any other reason that is required by PRC law

Through the extra-territorial nature of the PIPL's regulations, organisations operating outside of the PRC may still be applicable to comply with PIPL data processing rules, given that the organisation meets certain conditions, such as processing personal data originating in the PRC.

Definitions

'**Personal information**' within the PIPL includes any data points that relate to a natural person, excluding data that has been anonymized (PIPL, 2021).

'**Sensitive personal information**' within the PIPL includes information that could lead to a violation of an individual's dignity or personal or property safety. Such data points include religious beliefs, health records, geolocation, minors' data, and biometrics. This category of data points is comparable to the GDPR's 'special category' of data, which is restricted.

'**Personal information processor**' (**PIP**) within the PIPL means an individual or organisation that independently decides on the purposes and means of processing personal data. The PIP is comparable to the 'processor' within the GDPR, or the 'business' within the CPRA.

'**Important**' data is referred to by the Identification Guideline to be any data that is in electronic form and could endanger national security and public interests when interfered with, leaked, damaged, or illegally used otherwise.

National Data Protection Authority

The primary authority of China's legal data protection environment is the Cyberspace Administration of China (CAC), which is responsible for coordinating, overseeing, and

enforcing data protection rules. With this said, many Chinese agencies have held jurisdictional roles in data protection cases in the past, and will likely continue to be involved in a relevant way. These authorities are the following:

- Ministry of Industry and Information Technology, (MIIT)
- Ministry of Science and Technology
- Ministry of Public Security
- National People's Congress Standing Committee
- The State Administration for Market Regulation

The National Information Security Standardisation Technical Committee of China (TC260) publishes best practices, principles and standards for topics ranging from data privacy to cybersecurity. TC260 is an important agency in establishing the technical standards by which organisations are obliged to adhere with, across sectors.

There are also local branches of the Public Security Bureau as well as industry regulators, which hold roles in both managing and enforcing data protection regulation. There also exist regulators in main sectors, e.g., the People's Bank of China who aids in regulation of the financial sector.

Registration

The data protection laws of the PRC do not impose a requirement to register with a data protection authority before being permitted to process data. With this said, there are registration obligations of the disclosure and transfer of specified categories of sensitive data.

Data Protection Officers

The PIPL imposes a requirement upon organisations to designate a data protection officer and pass on the person's contact details to the respective data protection authority (PIPL, 2021). This requirement is dependent on the volume of data being processed by the organisation –

Article 52 asserts that if organisations process a certain volume of data, which is over the threshold set forth by the CAC, the organisation is obliged to appoint a DPO. As of April 2022, the CAC has yet to publish such threshold values.

Organisations that process the personal data of PRC residents and are based outside of the country, must appoint a representative or otherwise service provider within the PRC to register their contact with the data protection authority and be the point of contact for data protection activities.

Although PRC authorities haven't yet announced the data volume threshold for representative requirements, the Personal Information Security Specification (PISS) specifies requirements for appointing such representatives, when:

- The organisation's main activity is processing data & employs more than 200 individuals
- The organisation processes personal data of more than 100,000 unique individuals
- The organisation is estimated to process personal data of more than 1 million individuals

Data Collection & Processing

Consent

Before personal data may be collected, express and informed consent is required from data subjects. For activities involving sensitive personal data, like processing, cross-border transfers, or direct marketing, explicit consent is needed from the data subjects.

The PIPL imposes a further requirement of separate consent for:

- Processing sensitive personal information
- Data transfer to third countries
- Publicly disclosing personal information

- Providing data to a different controller for processing purposes
- Using imaged identification data collected in public for purposes other than public security

The concept of separate consent made its introduction in the PIPL and the meaning will likely be clarified by the CAC in the future, as with many of the aspects of the PRCs new data protection laws. With that said, separate consent can be understood to be explicit consent that is not bundled together with other notices in a privacy policy, but rather be a separate consent specific to the given purpose.

Consent from data subjects is not always required, and the PIPL specifies the circumstances where processing personal data without consent is lawful:

- Completing human resources data processing activities under legally established employment policy
- Joining or completing a contract with the data subject
- Carrying out processes in relation to legal obligations
- For reasons spanning public security and interest
- As obligated by any PRC law

Despite the PIPL's assertion of the legal bases upon which lawful data processing may take place, consent continues to be the primary legal basis for lawful data processing, as the reliance on the above bases is not yet clear.

Notice

Along with consent, the PIPL asserts the requirements of privacy policies, or other forms of notice be provided to data subjects before collecting and processing their data. Such notice should provide the scope of the data to be collected, as well as the ways it will be processed and disclosed. The required content that be included in notices to data subjects is:

- Identification & contact information of the data controller
- The personal data points to be collected along with the respective purposes
- The data retention period, location of data storage, means of processing
- The comprehensive purposes for which the controller needs the data (as with other regions, new purposes will require additional consent)
- The cases in which the controller transfers or discloses personal information to third-parties or otherwise publicly shares the data (Should include data categories, potential recipients, and the legal responsibilities of recipients)
- The potential risks and effects of providing the requested personal data points, or not providing such data points
- The rights of the data subject and clear methods that allow the exercise of such rights
- The state of data security made up by protection measures used by the controller, and the presence of compliance certificates when applicable
- Processes enabling data subjects to make inquiries and complaints, as well as providing data protection authority contact details

Further than providing all of the above information in notices to data subjects, the PIPL asserts that the content must be complete, true, accurate, and be clear & easy to understand. This privacy policy must be provided to data subjects upon collecting consent – and should remain easily and publicly accessible. Changes in the privacy policy should also trigger notifications to data subjects informing them of the modifications, and, where applicable, additional consent could be required.

Processing Principles

The PIPL requires that any use of personal data should always be directly linked with the purpose stated in the initial privacy policy, similar to GDPR's purpose minimization principle.

It also targets exorbitant data collection practices through the principle of data minimization. The use of biometric data collected in public remains restricted as well.

Impact Assessment and Documentation

Controllers are obliged to conduct personal information impact assessments (PIIA), and retain the results for 3 years when:

- Processing sensitive personal data
- Designating a separate data processor
- Sharing personal data with any third party
- Using personal data for automated decision-making processes
- Publishing personal data available to the public
- Transferring personal data to third countries
- Processing activities which could have significant effects for data subjects

The PIIA is required to assess the following aspects of processing activities:

- Evaluation of the purposes of data usage & whether the processing is necessary, legitimate and properly conducted
- Potential consequences and the effects to the interests of data subjects
- Suitability of security measures

Data Transfer

In the case that a controller wishes to disclose and effectively transfer personal data to third parties, the controller must abide by the following:

- Collect expressed prior consent & notify the subject of the purposes and recipients of the transfer
- Conduct a PIIA and based on the results, implement measures to protect subjects, i.e., a data transfer agreement

- Only transfer personal data which is required for the respective processing purposes
- Not disclose or transfer any categories of sensitive personal data where restricted by relevant law
- Accurately document the data relating to the transfer, including the purpose, scale, date, and information regarding data recipients
- Establish contractual measures between the processor and controller in order to cooperatively comply with obligations imposed by data protection laws

Cross-Border Data Transfer

The PIPL clarifies that in most cases personal data can be transferred to third countries, if the organisation has implemented the following steps of compliance:

- At least one of the following:
    - Cleared a CAC security evaluation
    - Certified by CAC-accredited agency
    - Implemented CAC standard contractual clauses with data recipient; or
- Compliance with each of the following:
    - The completion of a PIIA
    - The controller implements appropriate measures with the data recipient to ensure continued compliance with PIPL data processing rules
    - Notice to, in combination with separate, explicit consent from data subjects

Although the PIPL does not set forth general requirements of retaining copies of personal data within the PRC, certain categories of data are subject to data localisation requirements. This includes, but is not limited to:

- Personal information that is processed by operators of critical information infrastructure (Unless CAC-certified)

- Personal information that is processed by controllers and exceeds the records of 1 million individuals (Unless CAC-Certified)
- Data regulated by industry-specific rules, such as genetic information
- 'Important data' of a given sector, location data, other restricted categories

The PIPL imposes further rules regarding the international transfer of personal data originating in the PRC:

- Controllers may not transfer personal data within China to foreign authorities unless approved by a designated Chinese authority
- Through the extent of the existence of international agreements ensuring fairness and mutual benefit, Chinese authorities can transfer personal data within China to foreign authorities on request
- A list of foreign organisations will be maintained, which denotes entities to which PRC organisations are prohibited from transferring personal data to

Security

Through requirements imposed by the PIPL, DSL, and CSL regulations, organisations must maintain confidentiality of personal data, and implement a security management system for this purpose. Such obligation includes establishing sufficient technical and organisational measures to prevent the unauthorised processing, damage, loss or destruction of personal data. Similarly to the GDPR, Chinese legislation requires that the degree of measures taken must be appropriate to the risk posed by potential damage. The CSL and DSL define the security measures which organisations must implement, as well as the guidelines and standards set forth by the TC260. The PIPL specifically obliges controllers to implement encryption or anonymization procedures, as well as access controls and required cybersecurity training.

Organisations are obliged to establish systems allowing individuals to make complaints or reports that must be managed and documented.

Through the CSL, the cybersecurity protection of information systems of network operators is dependent on the classification of the information system into 5 possible tiers, called the multi-level protection scheme, (MLPS). Organisations must evaluate their information systems and use relevant regulations and guidelines to determine the tiers in which its information systems fit in. The classification of the company's information systems must be filed with the Public Security Bureau, and depending on the tiers determined, assessment by third parties may be necessary. The table diagram below summarises the five levels of necessary protection of information systems, based on the scope of effect and level of harm. Organisations must classify themselves into an appropriate category and adopt the technical standards of security required. (Hogan, 2019).

Controllers who appoint processors to process personal data for them are required to take actions to make sure the appointed entity maintains adequate security in order to protect the personal data. A data processing agreement between the controller and processor, which sets forth the processing rules, would be typical.

Breach notification

Each of the central data protection laws of the PRC impose requirements to notify authorities of data breaches, which are classified into 7 possible incident types. The China National Internet Emergency Center can provide advice on whether an incident should be reported or not, and other guidelines provide more information on this.

The process of reporting an incident includes the immediate notification to; the organisation's internal data protection officer, and the external regulator, including the following information:

- Causes and consequences of the incident

- Affected categories of data
- Corrective actions to minimise impact
- Contact details of the controller

The PIPL suggests that in cases when the controller is able to effectively mitigate the disclosure, loss, or modification of the data, data subjects need not be notified of the incident. When this is not the case, and the breach could damage the rights or interests of subjects, the CSL and DSL oblige the controller to immediately notify subjects. The yet to be, CAC-established, Personal Information Protection Departments (PIPD) may also assert to organisations that a breach could impact data subjects and request the notification of those data subjects. As above, similar information is required to be communicated to affected data subjects, along with counsel on protecting themselves from risks arising from the incident.

The Draft Network Data Security Management Regulation is a recent draft regulation, which supplements the PIPL and is expected to be used as a legal reference for enforcing data protection laws. Further conditions on data breaches are put forth by the regulation, requiring the notification of security incidents to the CAC and other authorities within 8 hours, including cases of:

- Data breaches including the personal information of 100,000 subjects or more, or
- Data breaches including any ‘important’ data

Following initial notification, another report has to be sent to the CAC within 5 days of the incident’s resolve. In all cases of suspected or actual security incidents, the organisation is required to take immediate steps of correction. Additionally, organisations are urged to put proactive measures in place, such as implementing a data incident contingency plan, or completing training across relevant roles.

Enforcement

The potential enforcement, and/or sanctions for a given data breach specifically depends on the laws infringed upon. The sanctions applied in a given data protection breach scenario vary widely across laws, and applicability varies across industries.

Non-compliance with the personal data protection rules of the CSL and PIPL can result in fines, confiscation of unlawful revenue, warning, or corrective measures. The fine assigned to the business may be up to CNY 1 million, where personal information protection officers deemed directly responsible face individual fines from CNY 10,000 to CNY 100,000. Cases of severe violation could include penalties such as the revocation of business licences, shutdown of websites, or suspension of business, and more. The PIPL includes another set of penalties for 'grave' cases of violation, where the organisation faces a fine of up to CNY 50,000,000 or 5% of annual revenue, and the directly responsible PIPOs face CNY 100,000 to CNY 1 million.

Criminal liability applies to people who sell or otherwise share the personal information of citizens to others, in violation of national laws. Penalties for such cases are grievous, with up to 3, or 7 years of imprisonment or criminal detention along with fines, all depending on the severity of the case.

Generally in the PRC, violations of personal data protection laws are prosecuted by public authorities, however according to interpretations of the criminal procedure law, individuals hold a private right of action e.g., in cases of individuals selling or providing personal data of other citizens to others.

E-Marketing

In the PRC, direct marketing towards individuals is only permitted when individuals have provided explicit consent.

Regulation imposes requirements on the content of direct marketing messages, such as the inclusion of the identity of the sending entity, and ‘Guang ago’ (Chinese for ‘advertisement'), or ‘AD’, to explicitly label the message as marketing. Aside from consent and the labelling of marketing messages, the sending entity is also obliged to disclose its identity and contact details, as well as providing an opt-out method in cases of electronic communications. Additionally, the nature of the direct marketing may not interfere or hinder the user’s normal usage of the internet, e.g., pop-up messages must include a conspicuously indicated ‘close’ mark.

Online Privacy

The general obligations of compliance for processing personal data set forth by the PIPL apply to offline contexts as well as online. The PIPL also categorises organisations into the following classes:

- Internet platform providers deemed ‘important’
- Controllers who perform large-scale processing of personal data
- Businesses deemed ‘complex’

The PIPL does not provide a clear explanation to guide which organisations fall into each category. Those respective categories are imposed to comply with additional obligations in processing personal data, as following:

- Establish personal data protection compliance processes
- Halt the offering of products if violations of data protection regulations are made
- Appoint independent and external data privacy organisations to supervise processes
- Implement and publish processing duties & rules regulating products in a fair way
- Regularly publish social responsibility reports on personal data processing
- Establish platform regulations

Furthermore, with regard to automated decision-making:

- Computer-based evaluation of behaviour, interests, hobbies, credit information, and more must be fair and open - discrimination among individuals is prohibited
- Forms of marketing should not aim at an individual's character, and should provide an easy method to opt-out

Additionally the PRC has in place the E-Commerce law and Consumer Protection law, offering protection to consumers' personal data (Protection of Consumer Rights Law, 1993). The obligations asserted by these laws include the bolstering of the administration of data granted by consumers, and the removal of infringing data, with required reporting to supervisory authorities. The need for sufficient notice and consent before processing personal data is also reiterated in these laws. Further duties are imposed upon mobile application providers, such as running real name identification, as well as conducting reviews of content on the app.

Regulators have focused on app providers in recent years and have published guidelines specific to them. These guidelines include data protection and privacy obligations towards mobile app providers in order to regulate collection and processing practices. There has been large-scale enforcement against infringing mobile apps, with the CAC reporting to have reviewed 1,425 of the most popular mobile apps in 2021 and issued obligations of corrective actions to 351 of those apps (Shen, 2021). The MIIT reported the removal of 540 mobile apps, as well as public obligations of corrective actions to 2,000 mobile apps, out of the 2.44 million apps it tested in 2021.

The rights of data subjects vested under PIPL and other relevant laws include the rights to access & obtain copies of their data, correct their data, erase their data in cases of data breaches, object to automated decision-making, and more. Also included is perhaps the

greatest right granted to individuals, the right to withdraw consent and thereby halt processing of their personal data.

The PRC has not set forth any regulations specifically applying to cookies, web beacons, or other online tracking mechanisms. With this said, the use of such technologies falls in the scope of processing personal information, and thereby relies on notice to and consent from data subjects.

The United States of America

Legislation

The United States does not have a single comprehensive legal framework in place for data protection. There is mostly sector-specific legislation at the federal level, while a few states have passed comprehensive data protection legislation independently. It should also be noted that numerous states now have similar comprehensive data protection laws in the legislative process.

Federal & State Privacy Laws

Federal data privacy legislation applies to healthcare providers, direct & electronic marketing, financial institutions, credit agencies, and driving records.

There are numerous state-level data protection and privacy laws which conflict with federal laws, some of which are preempted by the respective federal law.

Certain states have established data protection laws which go beyond federal law in including data security, online privacy, and breach notification regulations applicable across sectors. So far, state data privacy laws only safeguard the rights of residents of that state. Accordingly, businesses operating in the US must ensure compliance with applicable federal laws as well as the various state-level laws regarding data protection & privacy.

California is one of the states with the prominent data privacy laws with the California Privacy Rights Act (CCPA) introduced in 2018 (CCPA, 2018). This legislation was the first comprehensive data protection law to be applied across sectors and introduced broadly defined rights for individuals, while building considerable rules governing the collection, use, and sharing of personal data by businesses. The CCPA will soon be superseded by the Consumer Privacy Rights Act (CPRA) which comes into effect in 2023 and extends the CCPA by expanding consumer rights and asserting further rules on the use of residents' personal data (CPRA, 2020). The new legislation is also expected to have increased levels of enforcement through the establishment of a state enforcement agency to ensure compliance through the orders of corrective actions.

Colorado and Virginia have both followed California in developing and enacting comprehensive state data protection laws taking effect in 2023 (CDPA, 2021). These laws are considerably similar but are not identical, and vary from the CPRA. Where California's laws apply rules to personal data in professional contexts, Colorado and Virginia's do not, and the definitions and rules used in the CPRA vary substantially from the other state laws.

Farther than these three states, 16 others now have comprehensive consumer privacy bills in the legislative process. It can be expected that this trend will continue, and it could be possible that US Congress proposes to create a comprehensive data protection framework at the federal level, which would be comparable to the EU's General Data Protection Framework.

Consumer Protection

Consumer protection laws of the United States allow government agencies to penalise businesses for data protection & privacy violations.

The Federal Trade Commission (FTC)'s mission is to prevent business practices that are anticompetitive or deceptive or unfair toward consumers (FTC Act, 1913). Included in its

responsibility is taking enforcing actions and investigating entities for the following violations:

- Lacking the implementation of sufficient data security measures
- Misleading information or inaccuracies in privacy and security statements
- Failing to comply with the applicable self regulatory principles for a given industry
- Violating standards upheld by prior enforcement precedents through the unlawful collection, use, disclosure or otherwise failure to adequately protect personal information
- Disclose personal data to the acquiring entity of a merger, acquisition, or bankruptcy without having disclosed so in the privacy policy.

Select state attorney's general hold comparable enforcement power against unfair and deceptive business practices - covering violations of consumer privacy rights and insufficient security measures in their states. They also tend to cooperate on actions against companies that affect consumers across states, like a data breach including the personal data of residents of multiple states.

Definitions

The definition of '**personal information**' varies widely throughout US state and federal laws. Data security and breach laws, for example, define sensitive personal information as biometrics, financial account information, medical information and pieces of information that can lead to identity theft. Meanwhile, there are numerous state and federal laws which adopt a broader definition of personal information, as 'information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual' (NIST, n.d.).

The CPRA adopts a definition for **personal information** to be data that could be associated with, or otherwise relates to, describes, or identifies a consumer or their household, given that they are residents of California.

Colorado and Virginia privacy laws adopt a similar approach to California's definition of personal information, but exclude data points of professional contexts (CPA, 2021).

The meaning of '**sensitive personal information**' also differs by law and sector. An individual's medical, financial, credit rating, student, and biometric information are included, as well as online personal information of children younger than 13 and any data that could be used towards identity theft. Additional rules are applied to these categories of sensitive personal data.

The CPRA defines '**sensitive personal information**' to be a category of personal data which includes the following types of data points:

- Government ID information
- Financial account credentials
- Geolocation data
- Racial/ethnic origin or religious beliefs
- Content of a person's communications
- Genetic data

In addition to these types of data, California also rules personal information used in analyzing an individual's health or sex life as sensitive personal data - as well as processing biometric data in order to identify an individual.

The CPRA does not specify a meaning behind the '**data controller**', but uses the term '**business**' in a similar manner. California's 'business' is defined as any legal entity organised for the purpose of profit which collects personal information or otherwise chooses the purposes and the means of processing California residents' personal data. In order for the

CPRA to be applicable to a business, they need to either disclose or transact 100,000 California residents' personal information, or derive the majority of its revenue from selling personal information of California residents (CPRA, 2020).

The CCPA defines a '**data breach**' as cases when unencrypted personal data is or is reasonably believed to have been acquired by an unauthorised person, or in the same cases with encrypted personal data, where the encryption key was also believed to be compromised and could render the personal data readable.

National Data Protection Authority

There is no single enforcement agency for legal data protection violations across the nation.

The FTC issues and enforces federal privacy regulations over most commercial entities, with some exceptions being banks and insurance companies. Additionally, the FTC uses its authority to enforce against unfair & deceptive business practices that includes the umbrella of data collection and privacy malpractice (FTC Act, 1913).

About half of the state's attorney generals hold similar authority over 'unfair and deceptive practices', which includes inadequate security measures and violations of consumer rights where residents of their state are harmed.

Virginia, Colorado, and California's comprehensive state privacy laws are enforced by their state attorney generals. Once the CPRA is in force in 2023, the California Privacy Protection Agency (CPPA) will be established, an agency dedicated to monitoring compliance and enforcing the CPRA.

Registration

In the United States there are no requirements to register the processing activities or storage of personal information. However, California and Vermont are two states which impose rules on such data brokers. With the CCPA's 2019 amendment, data brokers are required to register

data processing activities with the attorney general of California. Data broker is defined to be a business intentionally collecting and selling personal information to third parties with whom the broker is not directly linked. Vermont's Data Broker Regulation requires data brokers in the state to register with the Vermont Secretary of State annually and provide specific information, while adhering to the minimum data security standards put forth by the statute (Data Broker Regulation, 2018). Similarly to California, Vermont's bill similarly defines data brokers as businesses intentionally selling personal data to third parties.

Data Protection Officers

In the United States there is no general obligation to hire a data protection officer within federal or state laws. However, those entities regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are exceptions. The HIPAA was built with the purpose to better the protection of patients' health information and requires organisations to hire one or more privacy and security officer(s) (HIPAA, 1996).

Additionally, numerous states have implemented laws that require the designation of employees to be responsible for and maintain the organisation's information security program. Massachusetts enacted this as a comprehensive Written Information Security Program (WISP) in 2010, with many states following suit since (WISP, 2010). Such programs can be seen as similar to appointing an officer for data protection, however the responsibilities and duties are not identical, where WISP is more focused on security measures.

Data Collection & Processing

Processing masses of personal information is the main focus of comprehensive data protection regulations like the CPRA. Generally,The common requirement amongst state privacy laws is

to provide a complete disclosure to individuals detailing the collection and use of their data and the relevant choices they have. With this the CPRA relies on an opt-out model where California residents continuously hold the right to opt-out of businesses selling their personal data to other entities.

Collecting and processing personal data is also regulated by US privacy laws and sector-specific principles. The common requirement in this facet is to provide a pre-collection disclosure to consumers detailing the collection and use of the data, as well as the relevant choices individuals have over their personal data.

Information categorised as sensitive data can in some cases require opt-in consent from the individual in order for lawful collection and use of the sensitive data. Types of data included in the meaning of sensitive data can be found in the Definitions section.

Both Colorado and Virginia's privacy laws impose a requirement on businesses to obtain consent from consumers at the time of data collection.

The Children's Online Privacy Protection Act (COPPA) restricts the use of minor's data, and requires verified consent of the parent before data may be collected. California's privacy acts go further to require businesses to obtain definitive consent before selling personal information of individuals which the business knows is under 16 years old, or expressive parental consent for individuals under 13 years old (COPPA, 1998).

When companies wish to use, share, or treat personal data in a manner which is incompatible with the initial purpose detailed in the privacy policy, the business must obtain additional consent from the individuals. The FTC asserts that changes to the purposes of usage of personal data collected are classified as retroactive material changes - and thus may penalise such cases .

The CCPA asserts that businesses collecting or using California residents' information must at least:

- Provide a privacy policy informing consumers of the:
    - Categories of personal information gathered & the categories which the business shares & those which have been sold in the past year;
    - Given purposes for the business collecting, using, and selling the data;
    - Categories of third party entities with whom the business discloses the data;
    - Categories of data sources from which the business collects the data;
    - Rights that consumers hold about their personal data & how to use them
- Provide two methods for individuals to file CCPA requests to the company
- Include a 'do-not-sell my information' link on the business homepage, which allows consumers to opt-out of the business selling their personal data
- Before or at the time of collection inform consumers of the categories of data to be collected and the respective purposes for collection

California's Shine the Light law and COPPA both assert further notice requirements for businesses, such that businesses must provide notice on whether they honour do-not-track mechanisms, as well as notice on whether they sell personal data to third parties for the purpose of marketing (Shine the Light Law, 2009).

Currently under the CCPA, individuals hold the right to request access to their personal information or erase it. In 2023 the CPRA, CPA, and Virginia CDPA state privacy laws will vest individuals with more rights - the right to correct their personal data records as well as participation in targeted-advertising. Furthermore, the bills impose requirements among businesses to conduct a risk assessment before taking part in certain high-risk processing activities, which relate to:

- Selling personal data
- Processing sensitive data types
- Unfair or intrusive profiling, targeted advertising purposes

Virginia's CDPA imposes a further requirement on businesses to create a process where, firstly, consumers are able to appeal a business's controller's denial of action on a consumer's privacy request. If the controller denies the appeal the consumer must have some accessible method to submit a complaint to the attorney general.

Many other states impose varying requirements, largely in the employee and student privacy areas. Additionally, there are numerous sector-specific laws which assert notice obligations, limit the allowed disclosures of personal data, and grant individuals with the power to access their personal data which a business holds.

Data Transfer

With the exception of certain government data, currently, the United States does not have in place any geographic restrictions on data transfers.

Data Security

The United States has different laws which impose obligations on businesses to take reasonable physical, technical and organisational measures ensuring the security of sensitive personal data. Some state laws assert more detailed requirements for data security.

As discussed in Data Protection Officers, Massachusetts first enacted a data security law in 2010 which required businesses to implement a written information security program. The regulation applies to companies collecting or maintaining sensitive personal data on residents of Massachusetts. Part of the bill asserts that any service provider who touches a business's sensitive data must also protect it in accordance with the law. Since Massachusetts being the first state to implement a data security law requiring a WISP, 25 US states currently legally require a WISP or similar solution (WISP, 2010).

Other states have imposed more requirements onto businesses, as with New York's SHIELD Act enacted in 2019 (SHIELD Act, 2019). This bill put in place minimum security

requirements for businesses collecting or using personal information, defined broadly as ID information, financial information, biometric data collected from facial recognition or other means, and e-mail information. The SHIELD Act requires businesses with personal data of NY residents to implement reasonable safeguards as set forth in the bill, designate at least one employee to coordinate the security program and report breaches, and regularly carry out risk assessments.

Certain sectors are regulated by other data protection laws which assert specific requirements on entities like in the health, insurance, and financial sectors. The Gramm-Leach-Bliley Act, for example, requires financial institutions in the US to implement appropriate security measures (Gramm-Leach-Bliley Act, 1999). State-level sectoral regulation is also present, where, for example, the New York Department of Financial Services sets forth substantial data protection and cybersecurity requirements on the financial & insurance businesses that are licencees of the department.

HIPPA's Security Rule established national standards for protecting individuals' electronic health data that was generated, received, used or maintained by a covered entity. Such a 'covered entity' is defined to include doctors, pharmacies, dentists, health insurance companies, Medicare, hospitals, as well as the 'business associates' that may interact with any personal health information on behalf of the entity (HIPAA, 1996).

Internet of Things

The United States has recently passed state and federal-level legislation regarding the Internet of Things (IoT). This recent law named the Internet of Things Cybersecurity Improvement Act of 2020, requires IoT devices purchased from, owned by, or controlled by federal agencies, to be used in compliance with best practices and security requirements set forth by the National Institute of Standards and Technology (NIST) (IoT Cybersecurity Improvement Act, 2020). Although the bill mainly applies to IoT devices used by the federal government,

its impact could lead to IoT manufacturers including secure technology and standards, ultimately making IoT devices more secure overall.

Breach Notification

The United States has federal laws in place imposing obligations of notice in the case of a data breach in the government, telecommunications, finance, and healthcare sectors.

All 50 of the United States, including Washington DC and Puerto Rico, have enacted breach notification legislation that requires notice be given to residents in the case that sensitive data is involved in a security breach. California was the first state to enact a breach notification law, with numerous other states following suit with similar legislation.

Additionally, California's CCPA and CPRA both impose obligations for businesses to notify any California resident whose personal data was compromised as a result of a data breach. California requires businesses to send a copy of the breach notification to the states attorney general when more than 500 California residents are affected (CPRA, 2020). The law requires the notification to include specific sections like 'What information was involved' and 'What you can do' - written in plain language and delivered without undue delay. Some of the states also impose obligations on the content and timeliness of the notices provided to state officials and to affected individuals.

Enforcement

Data protection laws and state privacy laws are enforced by different agencies in the United States. The authorities that take enforcement action include the FTC, the state attorneys general, and the sector-specific regulator (e.g., the Office of Civil Rights enforces the HIPAA data privacy laws applying to healthcare providers) (Health Information Privacy, 2013).

As mentioned in the Data Protection Authority section, California's CCPA gives individuals private right of action, meaning that they may sue a company in the case that the company

had a data breach exposing their personal data, without having put in place reasonable data security measures. The CPRA expands the private right of action which was granted to individuals in the initial CCPA. When the CPRA comes into effect in 2023, the categories of qualifying data will be expanded to include email accounts, meaning that if a data breach takes place where unencrypted records of email addresses together with passwords are leaked, the impacted individuals will have the right to sue for statutory damages. Database breaches containing such information as emails & passwords are increasingly common, and so this expansion translates to a greater risk of class action lawsuits where a group of victims may file suit against the responsible business.

Beyond the private right of action held by California residents, the state will enforce the CPRA through administrative penalties prescribed by the California Privacy Protection Agency (CPPA), the enforcement agency established as part of the CPRA. The CPPA will be responsible for offering guidance to businesses, making decisions on the time a business has to 'cure' alleged violations, and bringing enforcement action on non-compliant businesses through independent investigation, or through complaints of any persons. The potential administrative penalties are stated in the CPRA to be $2,500 for each violation or $7,500 for each intentional violation - or violations including the personal data of known minors.

The attorney general is also responsible for enforcing the CPRA through civil penalties of the same monetary values as the CPPA. Through a difference in wording, the attorney general of California does not need actual knowledge of the affected individuals' being minors when assigning penalties.

The CPRA does not give a ceiling limit for fines assigned to non-compliant businesses, which gives way to a large potential risk for companies processing masses of personal data. Beyond the financial impact is also the reputational damage, and loss of stakeholder trust, through violating the CPRA.

Three states, as well as HIPAA, have enacted cybersecurity safe harbour legislation, effectively protecting businesses from some of the penalties in case of a breach. The first state to set forth such a law was Ohio, which applies it most broadly – the Ohio Data Protection Act of 2018 offers companies a protection in the form of an affirmative defence against data breach cases where allegations include that reasonable security measures were not implemented beforehand. Ohio's law does not contain an exception for negligence as the alleged cause of the breach, which offers companies more protection (Ohio's Data Protection Act, 2018). Connecticut has most recently enacted a cybersecurity safe harbour law, where businesses are protected from punitive damages in cases alleging that the data breach was caused by a lack of reasonable data security, while the protection does not apply when the alleged cause is gross negligence.

E–Marketing

The United States has extensive marketing communications regulations in place, restricting marketing messages via fax, to SMS and more.

Email Marketing

The CAN-SPAM federal law of 2003 imposes requirements on all commercial emails in the United States (CAN-SPAM, 2003). It allows companies to send emails to any person, given that; the email includes the contact information of the company, the person has not already opted out of marketing messages from the company, and the message includes clear directions of how to freely and easily withdraw from commercial emails sent in the future. Those who violate the regulation on email marketing will be prosecuted by the FTC, the state attorneys general, or internet service providers.

SMS Marketing

Sending marketing messages to individuals' phones is regulated under both federal and state laws. In order for legal use of marketing messages to individuals' phones, expressive consent

from the receiving individual is required. This area has high potential of class action lawsuits and requires careful review of any marketing text messaging processes within a company to ensure compliance.

Marketing Phone Calls

Similarly, federal and state laws regulate the requirements on placing marketing phone calls to phones and making marketing phone calls using any autodialing equipment. In both of these cases, express consent of the individual is required prior to the call being placed. This is again an area of high risk, where companies that conduct heavy phone marketing need to ensure strict compliance of their practices.

Online Privacy

In the United States, federal law does not specifically restrict the use of cookies, web beacons and other online tracking mechanisms. State privacy laws apply to these tracking mechanisms, though, which impose an obligation of notice to individuals, and an option to opt-out of such tracking mechanisms.

Due to California's extensive definition of personally identifiable information, the data collected through web beacons, cookies, as well as targeted advertising activities would all be subject to the requirements of the CPRA.

California's privacy laws require that companies tracking personally identifiable information across websites over time must disclose whether they honour any do-not-track methods or otherwise provide an option to opt-out. There are further requirements on the disclosures required in the privacy policy in the case that third parties collect personal identifiable information on the company's website or others. Certain products and services are restricted from being advertised as well, such as alcohol, tobacco, firearms, and more.

Location Data

In the United States, notice to and consent from individuals is required in order to lawfully collect and process precise location data.

Region Comparisons

As a whole, the recent developments in data protection legislation across the US, EU, and PRC represent an acknowledgement of the importance of data security and the regulation of individuals' personal data. The legislation of the respective regions are, however, quite different, and illustrate different data protection landscapes. The EU took the first significant steps towards updating data protection legislation with the current times. The GDPR was indeed a significant step, and has since served as an example for future legislation across the world.

After the implementation of the GDPR, the forward-looking state government of California followed suit in implementing a comprehensive data protection law, through the CCPA and recent CPRA. With minor conflicts between state regulations, businesses may find trouble in complying with various state-level privacy laws. The inefficiency of conflicting patchwork state privacy laws has financial impact both on public taxes and on small businesses. The US is a global outlier in this aspect and should enact a bill that regulates the collection and processing of personal data across all states to increase productivity for the ecosystem.

The model used within the data privacy regulation by US states is for individuals to have the option to ‘opt-out’, perhaps the largest difference when compared to the GDPR’s ‘opt-in’ model. This difference gives EU citizens more rights towards their data, and reflects the high level differences between the two regions’ data protection laws. Individuals of the EU are given the right to choose the types of cookies they wish to allow, and give consent to companies requesting it. Through the CPRA individuals are required to be shown a detailed privacy notice explaining the use of their data, and their choices, such as opting-out of the sale

of their personal data. Another significant factor of each region's relevant legislation is the cross-border transfer of data containing personal information, which the US does not broadly restrict. The GDPRs application of common laws across Member States aims to further develop the EU's Digital Single Market in harmonising the digital market and its relevant components. Overall,This aims to accelerate the technology environment within Europe to push native businesses with growth, however some US businesses took the decision to exit the EU market rather than face the new conditions of compliance. Companies which are outside of the US and seek compliance with the applicable privacy laws likely do not need to take significant actions if they are already GDPR-compliant. Companies operating with US personal data should focus on the horizon of data protection bills and take proactive steps to be in compliance with the future of US data protection laws. Significant changes could come in the future – like New York's privacy bill introducing the opt-in model to the nation, and such changes need to be met with the implementation of new procedures to comply.

China has taken inspiration from the EU's regulation, and it can be seen with implementation of similar approaches across international data transfers, appropriate data security, and enforcement actions. Unlike the US, the EU and PRC both have implemented data protection laws which are inherently extra-territorial. With this, both regions regulate the circumstances when organisations may transfer data outside of its region of origin. The PRC goes further in building a publicly-available database containing a list of foreign organisations to which PRC-personal data is prohibited from transfer. With the case of companies processing data originating in the PRC or the EU, the respective region's authorities require a representative to be appointed within their region to serve as a point of contact. The EU and PRC's data protection laws also agree on the approach to security which organisations are required to comply with. Both regions' laws require security measures which constitute a level of security 'appropriate' to the risk of processing the personal data. They are almost identical approaches,

although China's Multi-Layer Protection Scheme (MLPS) gives way to a more straightforward understanding for organisations to self-evaluate their own tier and obtain the appropriate certification.

When compared to the current US patchwork of data privacy laws, the EU and PRC can be seen to give individuals stronger rights in regard to their data & how companies use it. The PIPL regulates automated decision-making in that it should be used with transparency towards the data subjects. In order to ensure equality of service, automated decision-making must not have in place any unreasonable measures that would discriminate against individuals in relation to transactional terms. Subjects in the PRC also hold the right to request an explanation of the purpose of their personal information in such situations. Much of these rights for individuals stem from the GDPR – rights to access, obtain, correct, or delete their personal data, not all of which are granted through US state privacy laws.

China's data protection framework is potentially the most challenging for companies to fully comply with. In the enforcement of the PIPL companies may face administrative, civil or criminal penalties, which include a reverse burden of proof forcing companies to prove their full compliance with PIPL through documentation. Given the range of required procedures to implement and more, documentation of the measures and procedures is key to success. Such main activities that require maintained documentation are the monitoring of personal data processing, the conducting of risk assessments, the development of rectification plans – continuous updates of consent documents, privacy policies, and data processing agreements. As well as these responsibilities are the required efforts to remain on top of China's regulatory developments, ensuring to remain in compliance with new technical standards and other requirements put forth. Businesses are permitted to appoint a data protection officer of their choice or contract a third party service provider to take care of the range of data protection activities.

Key Recommendations

In order for businesses to uphold compliance with a country's data protection regulations, workers must understand the key areas of compliance for the given region. Below are the highlighted areas of compliance which businesses must consider when operating with personal data from each region.

European Union

- Assess the applicability of regulations pertaining to VLOPs and 'gatekeepers'
- Check applicability & hire a data protection officer if obligated
- Implement procedures for notice and consent toward consumers
- Maintain detailed documentation of processing activities on personal data
- Examine the instances where the business is required to conduct a DPIA
- Implement procedures enabling the access, deletion, etc for data subjects' data
- Conduct GDPR compliance training for workforce of the business
- Fulfil cross-border data transfer obligations

The People's Republic of China

- Does your business require a dedicated representative in China?
- Classify the legal basis for each category of personal data used.
- Provide individuals with methods of withdrawing consent from processing
- Implement procedures enabling the access, deletion, etc for data subjects' data
- Implement mechanisms for security breach notifications
- Ensure cross-border data transfer requirements are fulfilled
- Gauge the need for PIIAs in accordance with the law
- Put processing agreements in place if working with third parties on processing

The United States of America

- Implement reasonable measures of data security for all processing activities
- Map the data of individuals and allow individuals to access, delete etc their data
- Assess the need for data protection assessments

- Examine the the need for data processing agreements, mainly when selling data
- Ensure the proper opt-out mechanisms are put in place for individuals to use
- Update privacy policy notice to include the extent of the required information

Appendix

Table 1: Differences in Consumers' Rights between the GDPR, CPRA, and PIPL (Cline & Li, 2021).

Provisions	EU's GDPR	California's CPRA	China's PIPL
Right to stop	Right to withdraw consent	Right to opt out of	Right to limit or refuse

processing	or otherwise stop processing of EU personal information	selling/sharing personal information; must include opt-out link on website	processing of personal information, with some exceptions; right to withdraw consent
Right to stop automated decision-making	Right to require a human to make decisions that have a legal effect	Regulations to govern access and opt-out rights for automated decision-making technology	Right to explanation and right to refuse solely automated decisions with significant impact
Right to stop third-party transfer	Right to withdraw consent for data transfers involving second purposes of special categories of data	Right to opt out of selling/sharing personal information to third parties	Requirement to obtain explicit consent before transfer to third parties
Right to equal services and price	At most, implicitly required	Explicitly required	Partial. Cannot refuse to provide goods and services if individual refuses to consent (unless necessary)
Regulator enforcement penalties	Ceiling of 4% of global annual revenues	No ceiling—$7,500 per violation	Ceiling of 5% of annual revenues or RMB 50m ($7.8m), plus potentially unlimited penalties to businesses and individuals

Table 2: State privacy law statuses in 2022 (IAPP, 2022).

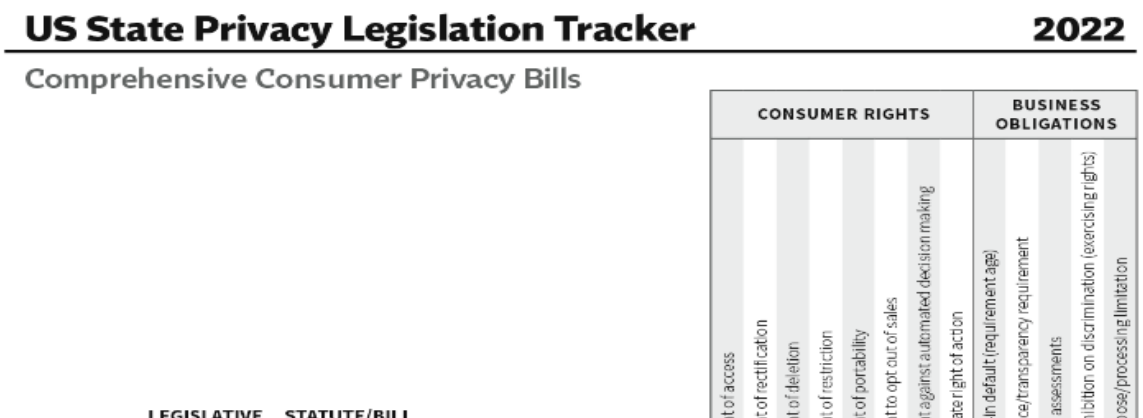
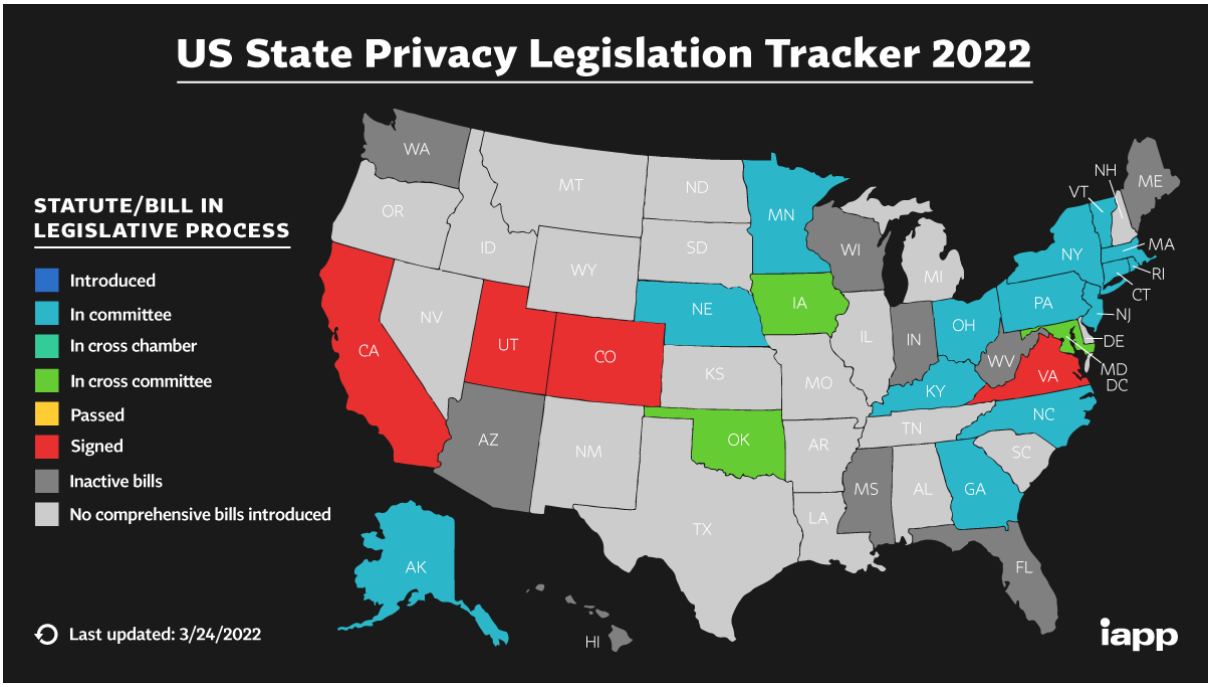


Table 3: Visualised map displaying the status of state privacy laws in 2022, (IAPP, 2022).


US State Privacy Legislation Tracker 2022
STATUTE/BILL IN LEGISLATIVE PROCESS
Introduced
In committee
In cross chamber
In cross committee
Passed
Signed
Inactive bills
No comprehensive bills introduced
Last updated: 3/24/2022
WA
OR
CA
ID
NV
MT
WY
AZ
UT
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
KY
TN
AL
OH
WV
GA
FL
SC
NC
VA
PA
NY
VT
NH
ME
MA
RI
CT
NJ
DE
MD
DC
AK
HI
iapp

References

Lewis, J. A. (2018). Table of Contents. In Rethinking Cybersecurity: Strategy, Mass Effect, and States (p. III–IV). Center for Strategic and International Studies (CSIS). Retrieved from http://www.jstor.org/stable/resrep22408.2

Das, R. & Gündüz, M. Z. (2019). Analysis of cyber-attacks in IoT-based critical infrastructures . International Journal of Information Security Science , 8 (4) , 122-133 . Retrieved from https://dergipark.org.tr/en/pub/ijiss/issue/67166/1048750

Slaughter, S. (2022). Cybersecurity Considerations Impacting the US Critical Infrastructure: An Overview. American Counterterrorism Targeting & Resilience Institute. Retrieved from https://americanctri.org/wp-content/uploads/2022/02/Cybersecurity-Considerations.pdf

Center for Strategic & International Studies (CSIS). (2018). In Rethinking Cybersecurity: Strategy, Mass Effect, and States. Center for Strategic and International Studies (CSIS). Retrieved from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Cohen, N. (2020). The Ethical Use of Personal Data to Build AI Technologies: A Case Study on Remote Biometric Identity Verification. Harvard Kennedy Center. Retrieved from https://carrcenter.hks.harvard.edu/files/cchr/files/200228_ccdp_neal_cohen.pdf

Meredith, S. (2018). Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal. CNBC. Retrieved from https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

National Academy of Engineering. (2019). Privacy and Security in the 21st Century: Who Knows and Who Controls?: Proceedings of a Forum. Washington, DC: The National Academies Press.https://doi.org/10.17226/25575.

Burri, M. (Ed.). (2021). Big Data and Global Trade Law. Cambridge University Press. Retrieved March 7, 2022, from https://doi.org/10.1017/9781108919234.

Eversheds Sutherland (US) LLP. (2018). California's GDPR Has Become Law. Retrieved from https://www.jdsupra.com/legalnews/california-s-gdpr-has-become-law-94942/

Office of the Attorney General: California Department of Justice (OAG). (2019). California Consumer Privacy Act (CCPA): Fact Sheet. OAG: California Department of Justice. Retrieved from https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf

Office of the Attorney General: California Department of Justice (OAG). (2019). California Consumer Privacy Act (CCPA). OAG: California Department of Justice. Retrieved from https://oag.ca.gov/privacy/ccpa

Congressional Research Service (CRS). (2019). Data Protection Law: An Overview. CRS. Retrieved from https://sgp.fas.org/crs/misc/R45631.pdf

Lewis, J. A. (2021). Towards a More Coercive Cyber Strategy: Remarks to U.S. Cyber Command Legal Conference. CSIS. Retrieved from https://www.csis.org/analysis/toward-more-coercive-cyber-strategy

Klosowski, T. (2021). The State of Consumer Data Privacy Laws in the US (And Why It Matters). New York Times. Retrieved from https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Boyne, S. (2018). Data Protection in the United States. The American Journal of Comparative Law. Vol. 66. Retrieved from https://academic.oup.com/ajcl/article/66/suppl_1/299/5048964

Lynn, T. (2021). Data Privacy and Trust in Cloud Computing. Springer. Retrieved from https://doi.org/10.1007/978-3-030-54660-1

Kontargyris, X. (2018). IT Laws in the Era of Cloud-Computing. Nomos. Retrieved from https://doi.org/10.5771/9783845295626

Jehl, L. (2018). CCPA and GDPR Comparison Chart. Bakerhostetler LLP. Retrieved from https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf

European Data Protection Supervisor (EDPS). (2018). The History of the General Data Protection Regulation. EDPS. Retrieved from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Papakonstantinou, V. (2022). Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity? Computer Law & Security Review. Retrieved from https://doi.org/10.1016/j.clsr.2022.105653

Banasiński, C. (2021). Cybersecurity of Consumer Products Against the Background of the EU Model of Cyberspace Protection. Journal of Cybersecurity, Volume 7. Retrieved from https://doi.org/10.1093/cybsec/tyab011

Graham, G. (2021). China's Completed Personal Information Protection Law: Rights Plus Cyber-security. Privacy Laws & Business International Report 20-23. Retrieved from https://dx.doi.org/10.2139/ssrn.3989775

Grotto, A. (2019). AI Policy and China: Realities of State-led Development. Digichina. Stanford Cyber Policy Center. Retrieved from https://cyber.fsi.stanford.edu/publication/ai-policy-and-china-realities-state-led-dvelopment

Chow, V. (2021). In the news: Hong kong cybersecurity review; social bond opening up; and US telecoms license ban. China Law & Practice, Retrieved from

https://ie.idm.oclc.org/login?url=https://www.proquest.com/trade-journals/news-hong-kong-cybersecurity-review-social-bond/docview/2597897477/se-2?accountid=27285

Mok, S. (2021). China's cybersecurity regulatory framework: A brief overview. China Law & Practice, Retrieved from https://ie.idm.oclc.org/login?url=https://www-proquest-com.ie.idm.oclc.org/trade-journals/chinas-cybersecurity-regulatory-framework-brief/docview/2584406821/se-2?accountid=27285

Brumfield, C. (2021). China's PIPL privacy law imposes new data handling requirements. CSO (Online), Retrieved from https://ie.idm.oclc.org/login?url=https://www.proquest.com/trade-journals/chinas-pipl-privacy-law-imposes-new-data-handling/docview/2566146649/se-2?accountid=27285

Mok, S. (2021). New heights in data protection: What companies need to know about china's data security law. China Law & Practice, Retrieved from https://ie.idm.oclc.org/login?url=https://www-proquest-com.ie.idm.oclc.org/trade-journals/new-heights-data-protection-what-companies-need/docview/2548451932/se-2?accountid=27285

Pernot-Leplay, Emmanuel. (2020). China’s Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?. Shanghai-Jiao-Tong-University. Retrieved from https://www.researchgate.net/publication/337103856_China%27s_Approach_on_Data_Privacy_Law_A_Third_Way_Between_the_US_and_the_EU

Bird, R. (2021). China “Standardises” AI Ethics. Freshfields Bruckhaus Deringer. Retrieved from https://technologyquotient.freshfields.com/post/102gpfp/china-standardises-ai-ethics

Walters, R., Novak, M. (2021). Cyber Security, Artificial Intelligence, Data Protection & the Law. Springer. Retrieved from https://doi.org/10.1007/978-981-16-1665-5

Article 101(1) TFEU. (2009). *European Antitrust Legal Text*. EU Antitrust Law. https://www.lexisnexis.com/uk/lexispsl/competition/document/391329/55KB-7MM1-F187-511S-00000-00/Article_101_1__TFEU_the_prohibition_on_restrictive_agreements_overview

CAN-SPAM. (2003). *CAN-SPAM Act Guidance*. CAN-SPAM Business Compliance Guidance. https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business

CCPA. (2018). *California State Government*. California Legislation. https://oag.ca.gov/privacy/ccpa

CDPA. (2021). *Virginia Consumer Data Protection Act*. Virginia Legislation. https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392

Cline, J., & Li, B. (2021, November 22). *How China's PIPL rules can impact your business*. PwC. Retrieved March 29, 2022, from https://www.pwc.com/us/en/tech-effect/cybersecurity/china-pipl-rules-impact.html

COPPA. (1998). *Children's Online Privacy Protection Act*. Code of Federal Regulations. https://www.ecfr.gov/current/title-16/part-312

CPA. (2021). *Colorado Attorney General Office*. Colorado's Attorney's General Office. https://coag.gov/resources/colorado-privacy-act/

CPRA. (2020). *California State Government*. California Legislation. https://cpra.gtlaw.com/cpra-full-text/

Data Act 2022/0047. (2022). *EU*. European Law Access. https://eur-lex.europa.eu/procedure/EN/2022_47

Data Broker Regulation. (2018). *Vermont Office of the Attorney General*. Guidance on Vermont's Data Broker Regulation. https://ago.vermont.gov/wp-content/uploads/2018/12/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf

Digital Markets Act 2020/842. (2020). *EU*. European Law Access. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN

Digital Services Act 2020/825. (2020). *EU*. European Law Access. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN

DSL. (2021). *13th NPC*. Chinese Law Access. http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml

FTC Act. (1913). *Federal Trade Commission*. FTC. https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act

Gramm-Leach-Bliley Act. (1999). *US Congress*. FTC. https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

Health Information Privacy. (2013). *Enforcement of HIPAA*. HHS.gov. Retrieved May 4, 2022, from https://www.hhs.gov/hipaa/for-professionals/faq/2019/who-enforces-hipaa/index.html

HIPAA. (1996). *HIPAA Summary*. HIPAA. https://www.cdc.gov/phlp/publications/topic/hipaa.html

IoT Cybersecurity Improvement Act. (2020). *H.R.1668*. Congress Search Engine. https://www.congress.gov/bill/116th-congress/house-bill/1668#:~:text=This%20bill%20requires%20the%20National,physical%20devices%20and%20everyday%20objects

NIST. (n.d.). *Personally Identifiable Information Definition*. National Institute of Standards and Technology. https://csrc.nist.gov/glossary/term/personally_identifiable_information

Ohio's Data Protection Act. (2018). *Ohio State Bar Association*. Ohio State Bar Association. https://www.ohiobar.org/member-tools-benefits/practice-resources/practice-library-search/practice-library/2019-ohio-lawyer/ohios-data-protection-act/

Ovide, S. (2021, October 12). *Big Tech Has Outgrown This Planet*. The New York Times. Retrieved May 6, 2022, from https://www.nytimes.com/2021/07/29/technology/big-tech-profits.html

PIPL. (2021). *13th NPC*. Chinese Law Access. http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

Protection of Consumer Rights Law. (1993). *12th NPC*. Chinese Law Access. http://www.npc.gov.cn/zgrdw/englishnpc/Law/2007-12/12/content_1383812.htm

Regulation 2016/679. (2016). *EU*. European Law Access. https://eur-lex.europa.eu/eli/reg/2016/679/oj

SHIELD Act. (2019). *Shield Act*. NY Senate. https://www.nysenate.gov/legislation/bills/2019/S5575

Shine the Light Law. (2009). *Shine the Light Law*. California Civil Code. https://law.justia.com/codes/california/2009/civ/1798.80-1798.84.html

WISP. (2010). *Written Information Security Program*. Massachusetts WISP. https://www.umassmed.edu/globalassets/it/documents/security/umms-wisp-2021.pdf

IAPP. (2022, April 28). *US State Privacy Legislation Tracker*. International Association of Privacy Professionals. Retrieved May 6, 2022, from https://iapp.org/resources/article/us-state-privacy-legislation-tracker/