Innovation & Tech Talk Online Event

China Cybersecurity Law, Data Security Law und Personal Information Protection Law

17. Februar 2022

ISACA
Germany Chapter

Presenter

Michael Morgenthaler

Datenschutzberatung, Dozent und CDPSE Trainer

Moderatorin

Sarah Richter

ADVISORI FTC GmbH

ISACA Germany Chapter

Hinweise

- Dieses Event wird aufgezeichnet und zusammen mit etwaigen Handouts nach der Veranstaltung auf www.isaca.de zur Verfügung gestellt.
- Eine CPE-Bescheinigung wird ca. zwei Wochen nach dem Event an die von den Teilnehmern bei der Registrierung angegebene E-Mail-Adresse versendet.
- Fragen an den Presenter oder Moderator können über die Chat-Funktion gestellt werden.
- Feedback zum Event, Anregungen oder Wünsche bitte an: fg-innovation@isaca.de
- Der nächste TechTalk findet am 31. März 2022 statt: www.isaca.de/veranstaltungen (in Kürze wird die Anmeldung veröffentlicht)
- Unser Podcast ist mit den ersten beiden Folgen verfügbar: www.isaca.de/Podcasts

ISACA Germany Chapter

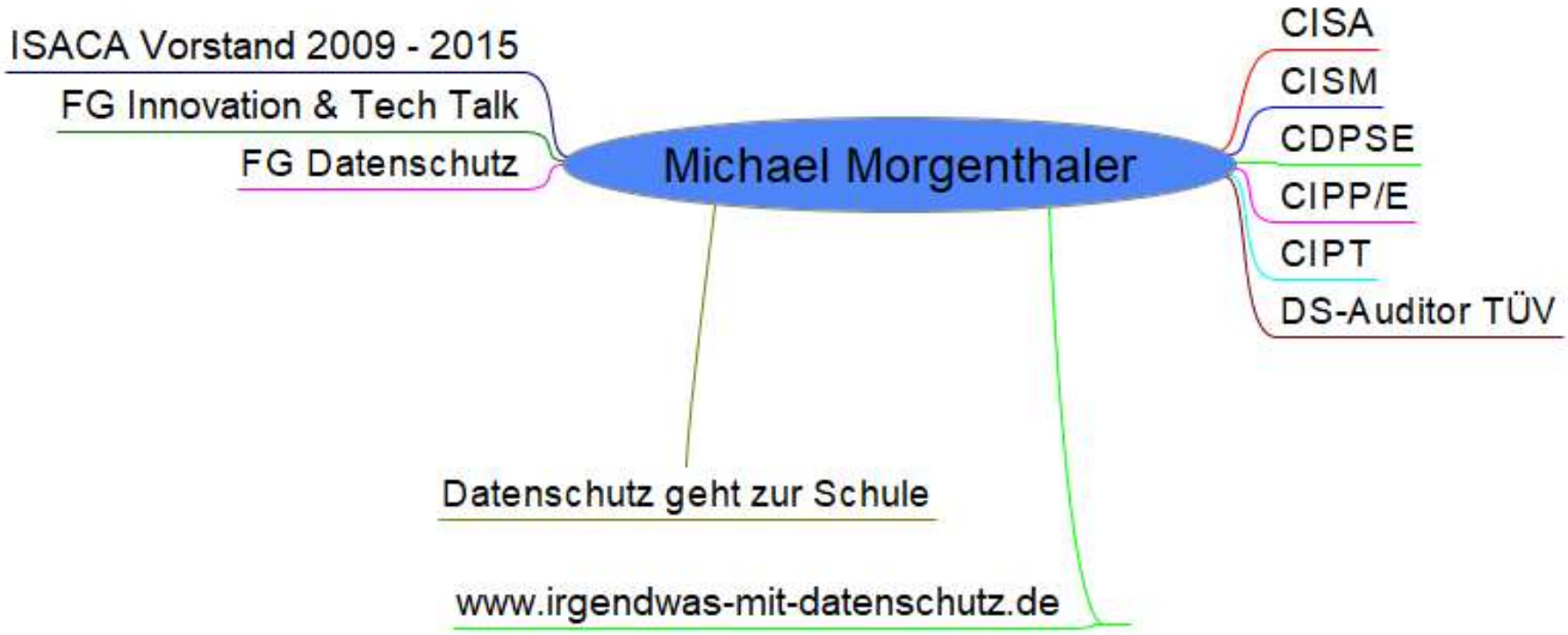
ISACA®

Germany Chapter

Cybersecurity, Data Location & Privacy

Michael Morgenthaler, 17.02.2022

Source Pixabay – Gerd Altmann


ISACA Vorstand 2009 - 2015
FG Innovation & Tech Talk
FG Datenschutz
Michael Morgenthaler
CISA
CISM
CDPSE
CIPP/E
CIPT
DS-Auditor TÜV
Datenschutz geht zur Schule
www.irgendwas-mit-datenschutz.de

Overview

01

Regulatory Landscape

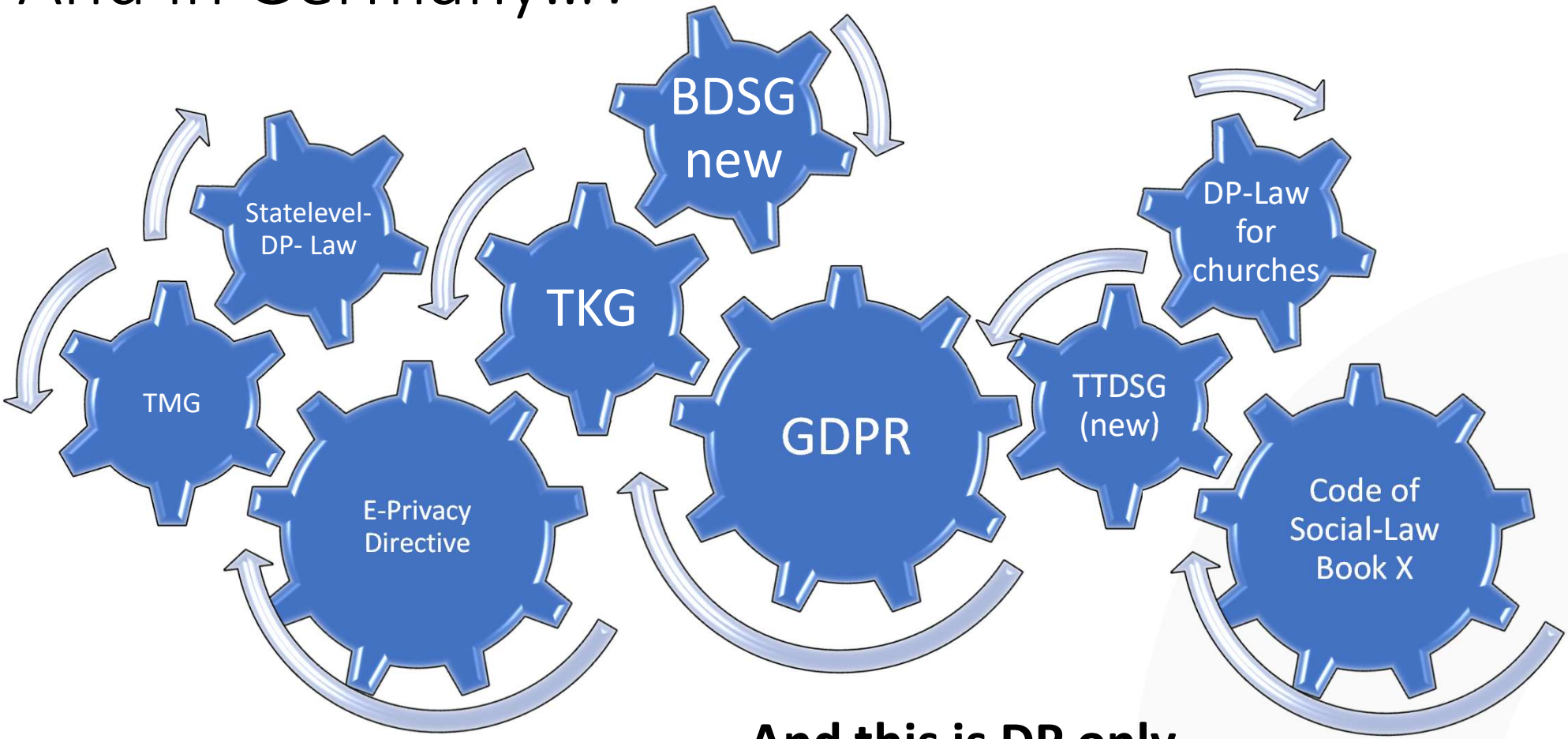
	Cybersecurity Law	Data Security Law	Personal Information Protection Law
Short	CSL	DSL	PIPL
1st draft	June 2015	June 2020	April 2021
Decided on	Nov 7th, 2016	June 10th, 2021	August 20th, 2021
In force	June 1st, 2017	September 1st, 2021	November 1st, 2021
Focus	**Security** of infrastructure and data handling	**Important Information** storage and exchange	**Personal Information** processing
German equivalent	IT-Sicherheitsgesetz	Not applicable	DSGVO / BDSG
Regulator	Cyberspace Administration of China (CAC) / Ministry of Public Security (MPS)	National Security Council (NSC)	Cyberspace Administration of China (CAC) (?)

Regulatory Landscape

	Cybersec		nal Information tection Law
Short	CSL		
1st draft	Jun		21
Decided on	Nov 7th, 2		20th, 2021
In force	June 1st		2021
Focus	**Security** of infrastr and data handling	a ge	**sonal Information** essing
German equivalent	IT-Sicherheitsgesetz	pplicab	DS O / BDSG
Regulator	Cyberspace Administration of China (CAC) / Ministry of Public Security (MPS)	ional Securit Council SC)	Cyberspace Administration of China (CAC) (?)

Jan 2022: **Internet Information Service Algorithmic Recommendation Management**
(Draft: 09/2021 / in force: 03/2022)

And in Germany…?



And this is DP only…

Cybersecurity Law 2017

02

Scope

Business affected

- Network operators
- Critical information infrastructure Operator (CIIO or CIO)
  - Public telecommunications or information service, Water, Energy, Transport, etc.
- Supplier of network products and services

Technical View

- Technical Infrastructure
  - **Network**: a system of computers or other information terminals and related equipment which, in accordance with prescribed rules and procedures, will collect, store, transmit, exchange and process information
- Applications

Scope

Cybersecurity Art. 76(2) using necessary means to:

(i) prevent attack, interference, destruction or illegal use or incidents of networks;
(ii) so as to maintain the reliability and stability of their operation and to safeguard the completeness, confidentiality and usability of "network information".

Critical information infrastructure (Art. 30)

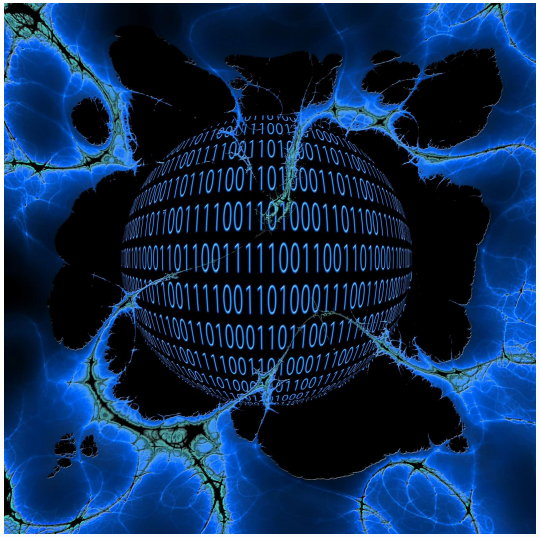
Destruction, loss of functions, data breach may seriously endanger national security, livelihood, economy, public interest of China

- definition of "critical information structure“ is missing

Provisions

Network operators

- Introduce and document internal operational procedure
- Establish Security Officer
- Protect against viruses, cyber attacks and invasion
- Recording/monitoring network incidents (logs)
- Security Incidents (Rresponse) Plans
- Data Classification needed
- "important data": backup procedures and encryption
- Notify supervisory authority in case of incidents

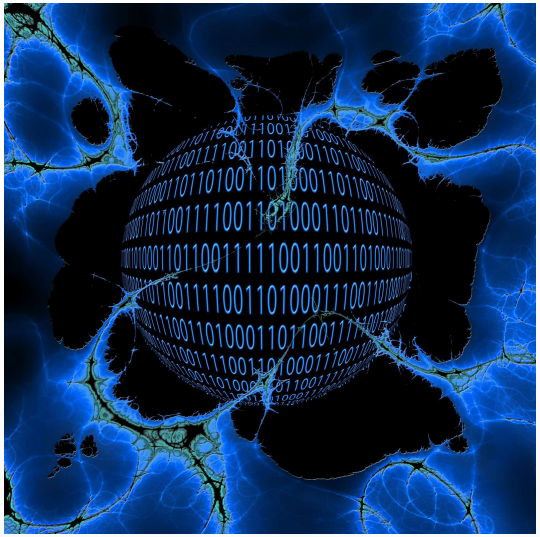


Source Pixabay – Gerd Altmann

Provisions

CIIO or CIO

- All from network operators
- Network security personnel
- Has to educate & check its workforce
- Establish backup systems for Critical system & database
- Security contingency plan with testing
- Written agreements with network product & service provider
- Procurement of network products and services must pass national security check
- Regular Audits needed



Source Pixabay – Gerd Altmann

Personal Information under Cyber Security Law

Definition

(i) information recorded electronically or otherwise, from which the identity of a natural person can be identified, either on its own, or combined with other information
(ii) personal identification information of a natural person includes the name, bitrth date, ID number, personal biometric information address, telephone number etc

Network operators must

- Establish "personal information protection system"
- Collection and use: principles of "legal, proper and necessary"
- Expressly notifies purpose + means + scope
- Must obtain consent
- Collection and use: make the relevant rules publicly available
- Direct marketing –consent
- Security breach notification
- Rights of citizens to access and request correction

CII/CIO must additionally

- store personal information collected or generated during operation in China (**Article 37**)

Data Security Law 2021

03

Overview DSL

Scope

- applies to data handling activities conducted within the territory of China and the security supervision and administration over such activities.
- has certain extra-territorial application for activities conducted outside the territory of China
- Establish “hierarchy” of responsible regulatory bodies

Overview DSL

Core Definitions (article 3)

- “data” refers to any information record in electronic or other form.
  - “important data” : the DSL requires the central government to publish a national-level catalog of “important data” and calls for regional and sectoral regulators to issue more detailed catalogs to further identify the scope of “important data” in their regions and sectors
  - **Art. 21** “Data related to national security, the lifelines of the national economy, mportant aspects of people’s livelihoods, major public interests , etc., constitute **core national data**

- “Data handling” includes the collection, storage, use, processing, transmission, provision, disclosure, etc., of data
- “Data security” refers to ensuring data is in a state of effective protection and lawful use through adopting necessary measures, and to possessing the capacity to ensure a persistent state of security

Chapter III Data Security Systems

Obligations for the state to…

- Establish a hierarchical data classification system (**Art. 21**)
- Provide hierarchical and classified protection for data
  - Importance of data in economic/social development
  - Harm to national security
  - Legitimate rights and interest of individuals
  - …
- Coordinate regions, departments and industries when formulating Important Data Catalogues
- Establish a centralized and integrated, highly effective, and authoritative mechanism for data security risk assessment, reporting, information sharing, monitoring, and early warning (**Art. 22**)
- Establish data security emergency response mechanism (**Art. 23**)
- Implement export controls in accordance with law for data belonging to controlled categories (Art. 25)

Chapter IV Data Security Protection Obligations

Obligations for the companies to…

Art. 27

- Establish data security management system
- Organize data security trainings
- Ensure data security by technical measures
- Establish MLPS 2.0 compliant classification
- Designate a person responsible for data security

Art. 28

- new data technologies shall be beneficial to promoting economic and social development, enhance the people's well-being, and conform to social morals and ethics

Art. 29

- Develop data security monitoring
- Take remediation action when security shortcomings are observed
- Have response plan available and initiate in timely manner

Art. 30

- Setup processes for risk assessment, documentation and submission to authorities

Chapter IV Data Security Protection Obligations II

Obligations for the companies to…

Art. 31

- Adhere to cross border transfer rules of Art 37 CSL when Important Data in scope
- Divided measures if CII or non-CII

Art. 33

- intermediary services provider shall
  - require the party providing the data to explain the source of the data,
  - examine and verify the identities of both parties to the transactions
  - retain verification and transaction records

Art. 36

- When foreign authorities request disclosure of data
  - Inform competent authority
  - Ask for approval from authority

Chapter VI Legal Liabiltv

- Warnings, sanctions and fines are outlined in **Art 44 – 52** detailing the responsibly entity and the misconduct acc. DSL articles
- Companies and individuals can be in scope of such measures

Compliance item	Monetary penalties	
	on companies (≤ yuan)	on directly responsible persons in charge (≤ yuan)
1 Establishment of data security management system[21]	2 million	200,000
2 Data risk monitoring and incident response obligations[22]	2 million	200,000
3 Important Data[23]: Designation of responsible person and etc.; regular risk assessment	2 million	200,000
4 Core Data[24]	10 million	/
5 Cross-border transfer[25]	10 million	1 million
6 Domestic enforcement cooperation[26]	500,000	100,000
7 Data request by foreign judicial or law enforcement agencies[27]	5 million	500,000
8 Data transaction (intermediaries) [28]	1 million	100,000

Zhong Lun: China's Data Security Law: Analysis and Compliance Guidance
https://mp.weixin.qq.com/s/qYmHwezeIYNI92TAyzfo6g

Personal Information Protection Law 2021

04

LinkedIn is shutting down its China platform because of a 'challenging operating environment'

By Rishi Iyengar, CNN Business

Updated 0810 GMT (1610 HKT) October 15, 2021

https://edition.cnn.com/2021/10/14/tech/linkedin-china-exit-microsoft/index.html

TECH

Yahoo pulls out of China, citing 'challenging' environment

PUBLISHED TUE, NOV 2 2021•7:25 AM EDT | UPDATED TUE, NOV 2 2021•8:47 AM EDT

https://www.cnbc.com/2021/11/02/yahoo-pulls-out-of-china-amid-challenging-environment.html

Personal Information Protection Law

- aims to "protect the rights and interests of individuals," "regulate personal information processing activities," and "facilitate reasonable use of personal information" (**Art. 1**)
- Fits with the new economic development strategy:
  - growth has to be sustainable, beneficial for society and helpful to economic upgrading.
  - growth will in future only be possible when it is good for the Chinese nation.
- could pave the way for China to obtain an "adequacy decision" under the GDPR, which is a prerequisite for allowing data transfers between the EU and other jurisdictions. (quote from Stephen Wong Kai-yi, Hong Kong's former privacy commissioner)

Chapter I: General Provisions
Chapter II: Personal Information Handling Rules
Chapter III: Rules on the Cross-Border Provision of Personal Information
Chapter IV: Individuals' Rights in Personal Information Handling Activities
Chapter V: Personal Information Handlers' Duties
Chapter VI: Departments Fulfilling Personal Information Protection Duties and Responsibilities
Chapter VII: Legal Liability
Chapter VIII: Supplemental Provisions

Definitions

The definition of **personal information** and **processing of personal information** are defined similarly under both of the PIPL and the GDPR.

> **Art. 4:** Personal information is all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, **not including information after anonymization handling**.
>
> Personal information handling includes personal information collection, storage, use, processing, transmission, provision, disclosure, deletion, etc.

Definitions II

Sensitive personal information is defined under the PIPL as “personal information that, once leaked, or illegally used, may easily infringe the dignity of a natural person or cause harm to personal safety and property security, such as biometric identification information, religious beliefs, specially-designated status, medical health information, financial accounts, information on individuals’ whereabouts, as well as personal information of minors under the age of 14” (**Art. 28 - 32**).

Definitions III

- **personal information processing entity (or Personal information handlers):** organization or individual that independently determines the purposes and means for processing of personal information (**Art. 73**).
  - ~ Chinese law equivalent of the “data controller” concept under the GDPR.
  - Obligations outlined in **Art. 52 - 59**
- **entrusted party (or entrusted person):** “data processor” as defined under the GDPR.
  - Entrusted persons shall handle personal information according to the agreement; they may not handle personal information for handling purposes or in handling methods, etc., in excess of the agreement. (**Art. 21**)
  - If the entrusting contract does not take effect, is void, has been cancelled, or has been terminated, the entrusted person shall return the personal information to the personal information handler or delete it, and may not retain it.

Lawful basis for processing needed (Art. 13, 14, 15)

Consent: it must be informed, freely given, demonstrated by a clear action of the individual, and may later be withdrawn

Separate consent required for certain processing activities, namely if a processing entity (i) shares personal information with other processing entities; (ii) publicly discloses personal information; (iii) processes sensitive personal information; or (iv) transfers personal information overseas

PIPL does not provide **legitimate interests** as a lawful basis for processing as found in the GDPR

Source : Pixabay
Peggy + Marco Lachmann

Lawful basis for processing (Art. 13)

Article 13 of the PIPL offers the following **non-consent basis**:

- Necessary to enter into or perform a contract <…>
- Necessary to perform legal responsibilities or obligations.
- Necessary to respond to a public health emergency
- To a reasonable extent, for purposes of carrying out news reporting and media monitoring for public interests.
- Processing of personal information that is already disclosed by individuals or otherwise lawfully disclosed, within a reasonable scope in accordance with the PIPL.
- Other circumstances as required by laws.

Source : Pixabay
Peggy + Marco Lachmann

Purpose, Transparency , Responsibility

Art. 6 and 7: Personal Information shall

- be processed for a clear and reasonable purpose and related to this purpose
- Be limited to the smallest scope for realizing the purpose, excessive collection is prohibited
- The principles of openness and transparency shall be observed

Security and Responsibility

Art. 9: Personal information handlers

- shall bear responsibility for their data handling
- adopt the necessary safeguards for the security of the personal information

Source : Pixabay
Peggy + Marco Lachmann

Rights of the Individual (Art. 44-50)

Rigth to	PIPL	GDPR
Information	Yes	Yes
Access	Yes	Yes
Correction/ rectification	Yes	Yes
Object / restrict processing	Yes	Yes
Data Portability	Yes	Yes
Not to be subject of automated processing	Yes	Yes
To withdraw consent	Yes	Yes
Lodge complaint with authority	Yes	Yes

- Aligned with GDPR to a great overlap
  - Not as detailed as GDPR
  - Answers need to be timely, not within a dedicated time
- it remains uncertain how such rights under PIPL might be interpreted in practice.
- Individuals will have the right to bring lawsuits against processing entities if they reject the individuals' requests to exercise their rights

Crossborder Data Transfer vs Localization

PIPL extends its territorial scope to the processing of personal information conducted outside of China, provided that the purpose of the processing is:

- to provide products or services to individuals in China,
- to analyze or assess the behavior of individuals in China, or
- for other purposes to be specified by laws and regulations (**Art. 3**).

Offshore (foreign) personal information processing entities have to

- establish a dedicated office or
- appoint a designated representative in China for personal information protection purpose.

Source : Pixabay Gerd Altmann

Crossborder Data Transfer vs. Localization

Local Companies that wish to transfer information internationally (**acc. Art. 38 – 43**) will have to

- use state-approved contracts or
- receive certification of data practices by a state-approved body or
- undergo a security review by Chinese cyber regulators

Critical Information Infrastructure Operators and businesses handling large amounts of user data, generally are required to store data inside China.

Source : Pixabay Gerd Altmann

Crossborder Data Transfer vs Localization

A processing entity that plans to transfer personal information to entities outside of China is required to

- provide individuals with certain specific information about the transfers and obtaining separate consent,
- adopt necessary measures to ensure that the overseas recipients can provide the same level of protection as required under the PIPL
- carry out an personal information protection impact assessment

Source : Pixabay Gerd Altmann

Personal Information Protection Impact Assessment

- **Art 55, 56**: Carry out an personal information protection impact assessments prior any processing and retain the processing records for at least three years when:

- Processing of sensitive personal information.
- Processing of personal information for automated decision-making
- Entrusting vendors to process personal information, sharing personal information with other processing entities or publicly disclosing personal information.
- Transferring personal information overseas.
- Other personal information processing activities that may have significant impacts on the rights and interests of individuals.

Source : Pixabay
Peggy + Marco Lachmann

Fines

In case of violations of PIPL

- Regulators may order to take corrective actions, issue warnings, confiscate illegal income, suspend services or issue a fine.
- The fine can be up to 50 million RMB or 5% of an organization's annual revenue for the prior financial year (**Art. 66**)
- Besides monetary fines, violations may also be recorded into the "credit files" of the processing entity under China's national social credit system.
- The processing entities will be liable for tort damages if they infringe the rights and interests of personal information

Source : Pixabay
Peggy + Marco Lachmann

Additional Concepts

- **Art. 16**: not refuse service when individual does not agree to data handling
- **Art. 17:** Information notice to individual prior processing
  - **Art. 23**: Information when data is shared
- **Arti. 19**: Data retention for the minimum period needed acc. purpose
- **Art. 20**: Joint Information Handlers
- **Art. 52**: Appointment of a Information Protection Officer

Source : Pixabay
Peggy + Marco Lachmann

Impact

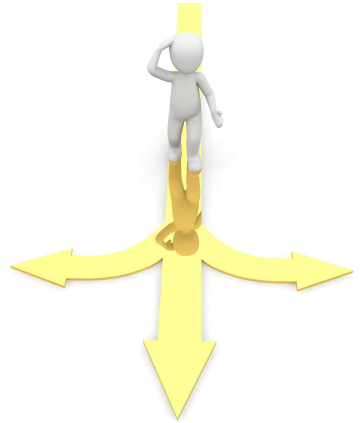
Business landscape to change!

PIPL will make tech giants lot less powerful and force many businesses to adapt as it will be much harder to legally collect and use consumer data.

Any company that relies on data to up sell you, sell data to others for advertising, or provide advertising services will have to change their business model.

The ban on algorithmic price discrimination is a key aspect.

- According to the law, if personal information is used in automated decision-making, the process has to be transparent and different individuals cannot be subject to different transaction terms.



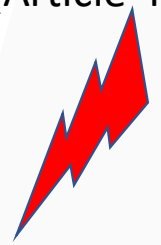
Source : Pixabay
Peggy + Marco Lachmann

Cyberspace Administration of China (CAC)

CAC is the lead agency that regulates activities in the cyberspace in China and takes the overall "coordination, supervision and management" role under the CSL, DSL and PIPL.

The CAC's role under PIPL:

- can issue general implementation rules and standards, as well as making specific rules in relation to sensitive personal information protection, facial recognition, artificial intelligence and other emerging technologies or applications (Article 62).
- issuing implementation rules regulating cross-border data transfer certifications and formulating standard contract to be entered into (Article 38).
- is designated as the lead agency that coordinates sectoral regulators and local government to enforce the PIPL (Article 60).
- will be the agency that administers the security assessment for the cross-border transfer of personal information by operators of CII or personal information processing entities that process personal information "in a volume that reaches the threshold to specified by CAC" (Article 40).



Ministry of Public Security (MPS)

Sources

- https://iapp.org/news/a/chinas-key-enforcement-agencies-and-lessons-learned-from-recent-actions/
- https://www.scmp.com/tech/big-tech/article/3146873/new-privacy-law-china-could-reshape-cross-border-data-rules-similar
- https://iapp.org/news/a/the-future-of-data-localization-and-cross-border-transfer-in-china-a-unified-framework-or-a-patchwork-of-requirements/
- https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/
- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3964684 **China's Emerging Data Protection Framework – University of Leiden 16.11.2021**
- https://www.china-briefing.com/news/china-passes-sweeping-recommendation-algorithm-regulations/ **Internet Information Service Algorithm Recommendation Management Regulations**

Thank You!

QUESTIONS?

Source : Pixabay
Peggy + Marco Lachmann