Organiser: BRITISH CHAMBER OF COMMERCE GUANGDONG 广东英国商会 | AUSTCHAM SOUTH CHINA A MEMBER OF AUSTCHAM GREATER CHINA 中国澳大利亚商会-华南

Partner: 中倫律師事務所 ZHONG LUN LAW FIRM | DEZAN SHIRA & ASSOCIATES Your Partner for Growth in Asia | GZAEFI 广州外商投资企业协会 Guangzhou Association of Enterprises with Foreign Investment

Data Protection & Network Security Measures for Companies in the Greater Bay Area—Legal and IT Consideration

Echo Ji

Events Manager

BRITISH CHAMBER OF COMMERCE
GUANGDONG 广东英国商会

BRITISH CHAMBER OF COMMERCE
GUANGDONG 广东英国商会

Joining the Dots

Your business link between the UK and South China

The British Chamber of Commerce Guangdong is an independent, non-profit organisation formed to facilitate and support Chinese and British companies operating in the PRD, now the GBA.

Promote

GBA Symposium

Share

Education Working Group

Supporting Members

Britannia International School 广州市英伦国际学校

CLYDE&CO

广州斐特思公学 Fettes College Guangzhou

MISSION HILLS CHINA

Partners

British Consulate-General Guangzhou

Department for International Trade 国际贸易部

CULTURAL AND EDUCATION SECTION OF THE BRITISH CONSULATE-GENERAL 英国总领事馆文化教育处

美通社 PR Newswire

- Branding, Marketing, Promotion Support
- Connectivity, Networking
- Business Matching Opportunities
- Event Cooperation/ Co-Branding
- Knowledge, Information Sharing
- Privilege Club

Connect

BritCham in Your Neighborhood

Access

Business Luncheon with British Consul-General

BRITISH CHAMBER OF COMMERCE
GUANGDONG 广东英国商会

How we can help

- Events – Training, seminars, members-only events, socials, high profile speakers
- Marketing support – Helping business to promote what they do
- Referrals – bringing business together
- Access to UK Gov contacts, events and information

Follow us

www.britchamgd.com

BRITISH CHAMBER OF COMMERCE
GUANGDONG 广东英国商会

BritCham's Upcoming Events

Date	Time	Event	Location
24 Oct	18:00-21:30	Zhuhai Social Drinks	Zhuhai
27 Oct	14:00-21:30	Executive Dinner (Shenzhen)	Shenzhen
29 Oct	18:30-21:30	Executive Dinner (Guangzhou)	Guangzhou
7 Nov	11:00-17:00	British Day (Guangzhou)	Guangzhou
21Nov	11:00-17:00	British Day (Shenzhen)	Shenzhen
5 Dec	18:00-22:00	Christmas Party	Guangzhou

BRITISH CHAMBER OF COMMERCE
GUANGDONG 广东英国商会

Follow us!

BRITISH CHAMBER OF COMMERCE
GUANGDONG 广东英国商会

Speakers:

Matthew Warr
Legal Consultant
Zhong Lun Law Firm

Kent Woo
Partner
Zhong Lun Law Firm

Thomas Zhang
IT Director
Dezan Shira & Associates

中倫律師事務所
ZHONG LUN LAW FIRM

LEGAL SOLUTIONS FOR
CHINA BUSINESS

Personal Data Protection and Network Security Measures for Companies in the Greater Bay Area

Matthew WARR, Legal Consultant
Kent WOO, Partner
Zhong Lun Law Firm Guangzhou Office
22 October 2020, 2:00pm-4:30pm

Agenda

Part 1: Chinese Data Protection Laws - Some Basics

Part 2: Legal Obligations and Rights

2.1 Legal Obligations of Data Controllers
2.2 Legal Rights of Data Subjects
2.3 Restrictions on Electronic Marketing

Part 3: Forming Company Policies on Data Protection

3.1 Privacy Policy
3.2 Employee Privacy and Monitoring Policy

Agenda

Part 4: Data Breaches and Data Governance

4.1 Data Breaches: What to Do
4.2 Data Governance: Data Protection Officers

Part 5: Data Localization and Cross-Border Data Transfers

Part 6: Outlook and Developments

中倫律師事務所
ZHONG LUN LAW FIRM

PART 1: CHINESE DATA PROTECTION LAWS - SOME BASICS

Chinese Data Protection Laws - Some Basics (1)

Currently no single comprehensive data protection law in China.

Two important laws related to personal data protection:

- *Cyber Security Law* (in force since 1 June 2017)
- *Civil Code* (issued on 28 May 2020, will come into force on 1 January 2021)

An important national technical standard related to personal data protection:

- *Information Security Technology – Personal Information Security Specification* (latest version issued on 6 March 2020; in force since 1 October 2020) ("**PIS Specification**")

Note that the PIS Specification is not legally binding but is of great significant in practice and an important reference point for regulators.

Some sectors are governed by additional, stricter regulations.

Chinese Data Protection Laws - Some Basics (2)

Definition of personal information:

> "Various kinds of information that is recorded electronically or in any other form, and **independently or in combination with other information, can identify a specific individual,** including an individual's name, date of birth, ID card number, biometric information, address, mobile phone number, email, health information, and whereabouts etc.".

Reference: Civil Code, Art 1034

中倫律師事務所
ZHONG LUN LAW FIRM

PART 2: LEGAL OBLIGATIONS AND RIGHTS

Legal Obligations of Data Controllers

Companies that collect and use personal data/information have certain legal obligations, including:

- Having a lawful, justifiable and necessary purpose
- Obtaining consent
- Obtaining consent again if using data for new purposes
- Publicizing the rules for collection and use
- Expressly stating the purpose, method and scope of collection and use
- Minimization of collection and use
- Guaranteeing the security of the data
- Informing data subject and relevant authorities if data is divulged, falsified or lost
- Involving personal information subjects

Reference: Cyber Security Law, Art 41; Civil Code, Arts 1035, 1038

Individual Rights of Data Subjects

Individuals have certain legal rights in regard to their data, including the right to:

- Access data or copies of data
- Correction of errors
- Deletion of data
- Cancellation of accounts
- Withdrawal of consent

Reference: Cyber Security Law, Art 43; Civil Code, Art 1037; Provisions on Protection of Personal Information of Telecommunication and Internet Users, Art 9; Regulation for Identifying the Illegal Collection and Use of Personal Information by Applications (Apps), Art III(8); 2020 Information Security Technology – Personal Information Security Specification, Sections 8.2, 8.4

Restrictions on Electronic Marketing

Data subjects also have the right to object to marketing. Organizations/individuals must:

- Obtain consent of parties concerned before sending them advertisements or commercial information via electronic means.
- State in the advertisements the true identity and contact details of the sender, and the method for refusing acceptance of future advertisements.
- For emails, indicate the word “advertisement” or “AD” in the email subject.

Reference: Advertisement Law, Art 43; Consumer Rights Protection Law, Art 29; Administrative Measures for Internet E-mail Services, Art 13

中倫律師事務所
ZHONG LUN LAW FIRM

PART 3: FORMING COMPANY POLICIES ON PERSONAL DATA PROTECTION

Forming Company Policies on Personal Data Protection

Important company policies on personal data protection include:

- **Privacy policy**
- Data protection compliance policy
- Data leakage response policy
- **Employee privacy and monitoring policy**

Privacy Policy (1)

Privacy policy: A statement or a legal document that states how a company collects, uses, discloses and manages a customer's or user's personal information or data.

Why is it important? Because China's *Civil Code* and *Cyber Security Law* requires companies to obtain users' informed consent before collecting and using their personal information.

Top concerns of authorities in their assessment of a company's privacy policy include:

- Readability and understandability of privacy policy
- Description of purpose, method and scope of collecting and using users' personal information
- Necessity of collection and use of the personal information
- Security protection measures adopted
- Protection of users' rights

Privacy Policy (2)

Best practice when constructing a privacy policy:

- Easy to read and understand
- Easily found on website or app
- Regularly reviewed and updated
- Users timely notified of changes

Formulate and implement the privacy policy in accordance with the latest version of the non-binding PIS Specification (in force since 1 October 2020).

According to the PIS Specification, privacy policy should also include:

- Retention period
- Data controller's contract details
- Complaint procedures
- Anticipated transfers to third parties

Reference: 2020 Information Security Technology – Personal Information Security Specification

Employee Privacy and Monitoring Policy (1)

During recruitment:

- Employers are entitled to know the basic information of employees in direct relation to the labor contract, such as work experience, educational background, health check etc.
- Employers should avoid collecting personal information not related to the labor contract, such as marital status, family background etc.
- Employers should delete the personal information of candidates who were not recruited.

Reference: Labor Contract Law, Art 8

Employee Privacy and Monitoring Policy (2)

During employment:

- Employers may need to supervise/manage employees and monitor employees' activities/behavior.
- Employers may obtain images/videos of employees through cameras, fingerprints of employees through attendance machines, and information about employees' location through apps.
- Employers may also monitor work computer and email and collect/use information for international monitoring or investigation purposes.
- Employers must ensure that monitoring measures and personal information collected is for legitimate purposes and necessary for business operations.
- Employers must avoid monitoring employees and collecting their personal information outside working hours and workplace.

However – informed, written and signed consent of employees is required.

Written consent usually obtained through a provision in labor contract and/or employee handbook.

中倫律師事務所
ZHONG LUN LAW FIRM

PART 4: DATA BREACHES AND DATA GOVERNANCE

Data Breaches: What to Do

Where personal data is divulged, damaged, falsified or lost (or there is a potential for such incidents), information processors must:

- take immediate remedial measures;
- inform the individual(s) concerned; and
- report to the relevant government department(s).

Report should include the:

- type, quantity, content and nature of affected data subjects;
- impact of the data breach;
- measures taken or to be taken; and
- contact information of relevant persons.

Reference: Cyber Security Law, Art 42; Civil Code, Art 1038; 2020 Information Security Technology – Personal Information Security Specification, Section 9.1

Data Governance: Employing Data Protection Officers

No general requirement under Chinese "laws" for organizations to employ a "Data Protection Officer".

However, the **non-binding** PIS Specification requires organizations to employ full-time person(s) in charge of personal data protection (i.e., Data Protection Officer) and establish a **data protection department** if the organization meets any of the following conditions:

- Its main business involves personal data processing and has more than 200 employees;
- It processes the personal data of more than 1 million individuals;
- It expects to process the personal data of more than 1 million individuals within 12 months; and
- It processes the "sensitive" personal data of more than 100,000 individuals.

Note that there is a general legal requirement for organizations to employ "persons responsible for cyber security" (i.e., Cyber Security Officer).

Reference: Cyber Security Law, Art 21; 2020 Information Security Technology – Personal Information Security Specification, Section 11.1

中倫律師事務所
ZHONG LUN LAW FIRM

PART 5: DATA LOCALIZATION AND CROSS-BORDER DATA TRANSFERS

Data Localization and Cross-Border Data Transfers (1)

Three principle requirements for transferring personal data outside China:

1. Data localization
2. Data subject consent
3. Security assessment

Principles currently only apply to “Critical Information Infrastructure Operators”

What is CII and which companies are considered CII Operators?

> CII is: “infrastructure that, in the event of damage, loss of function, or data leakage, may seriously endanger national security, national economy, people’s livelihoods, or the public interest”

Reference: Cyber Security Law, Art 41

Data Localization and Cross-Border Data Transfers (2)

Companies operating in the following industries may be considered CII Operators:

- Public communications
- Information services (e.g., telecom networks, TV networks)
- Energy
- Transportation
- Water utilities
- Finance
- Public services
- E-government affairs
- Healthcare
- Education
- Environmental protection
- Scientific research and production in industries such as national defense, science and industry, chemical engineering, food and drugs

Reference: Cyber Security Law, Art 31; Regulations on the Protection of the Security of Critical Information Infrastructure, Art 18

Data Localization and Cross-Border Data Transfer (3)

Two draft measures further expand data localisation and data transfer security assessment requirements from CII operators to *all network operators.*

Other requirements under the 2019 Draft Measures:

- Establish data transfer agreements with all overseas data recipients
- Submit an annual report to the Cybersecurity Administration of China (CAC)
- Maintain a log of all cross-border transfers of personal information for at least 5 years
- Establish and maintain an effective incident response place and report all major data security incidents

How long does a security assessment take?

- Usually within 15 days, but may be extended in complex situations

Additional restrictions apply to transfers of certain types of data, including:

- State secrets
- Personal financial information
- Population and health information
- Data related to human genetic resources

Reference: 2017 Measures for Security Assessment of Cross-Border Transfer of Personal Information and Important Data (Draft for Comments); 2019 Measures for Security Assessment of Cross-Border Transfer of Personal Information (Draft for Comments), including Art 5

中倫律師事務所
ZHONG LUN LAW FIRM

PART 6: CONCLUSION: OUTLOOK AND DEVELOPMENTS

Conclusion: Outlook and Developments

Draft Data Security Law issued for public comment on 3 July 2020.

Draft Personal Information Protection Law is expected to be issued for public comment soon.

Recent campaigns and increased enforcement by authorities in relation to personal information protection breaches by APP operators.

中倫律師事務所
ZHONG LUN LAW FIRM

LEGAL SOLUTIONS FOR
CHINA BUSINESS

Thank You!

Contacts

Kent Woo
+86 20 2826 1777
kentwoo@zhonglun.com

Matthew Warr
+86 183 4456 0653
matthewwarr@zhonglun.com

DEZAN SHIRA & ASSOCIATES

Your Partner for Growth in Asia

Personal Data Protection and Network Security Measures for Companies in the Greater Bay Area - IT Considerations

Thomas Zhang, DPO/CISA/CDPSE/CISSP/CCSP

Oct 22, 2020

Table of Contents

Section 1

Concepts and Terminologies about Personal Data Protection

Privacy and Personal Data

- **Identity**
  - Identified individual
  - Pseudonym
  - Anonymity

- **Types of Personal Data**
  - Direct vs indirect personal data
  - First-hand vs 3rd party personal data
  - Sensitive personal data

- **Privacy and Privacy Management**

CSL

Table B.1 Examples of sensitive personal information

Personal property information	Bank account, authentication information (password), bank deposit information (including amount of funds, payment and collection records), real estate information, credit records, credit information, transaction and consumption records, bank statement, etc., and virtual property information such as virtual currency, virtual transaction and game CD Keys.
Physiological and health information	The records generated in connection with medical treatment, including pathological information, hospitalization records, physician's instructions, test reports, surgical and anesthesia records, nursing records, medicine administration records, drug and food allergy, fertility information, medical history, diagnosis and treatment, family illness history, history of present illness, history of infection.
Personal biometric information	Personal gene, fingerprint, voice print, palm print, auricle, iris, and facial recognition features, etc.
Personal identity information	ID card, military officer certificate, passport, driver's license, employee ID, social security card, resident certificate, etc.
Other information	Sexual orientation, marriage history, religious preference, undisclosed criminal records, communications records and content, contacts, friends list, list of chat groups, records of whereabouts, web browsing history, precise location information, accommodation information, etc.

GDPR

- ✓ data revealing racial or ethnic origin
- ✓ data revealing political opinions
- ✓ data revealing religious or philosophical beliefs
- ✓ data revealing trade union membership
- ✓ genetic data
- ✓ biometric data processed for the purpose of uniquely identifying a natural person
- ✓ data concerning health
- ✓ data concerning a natural person's sex life or sexual orientation

Security vs Privacy

Privacy is much broader than security

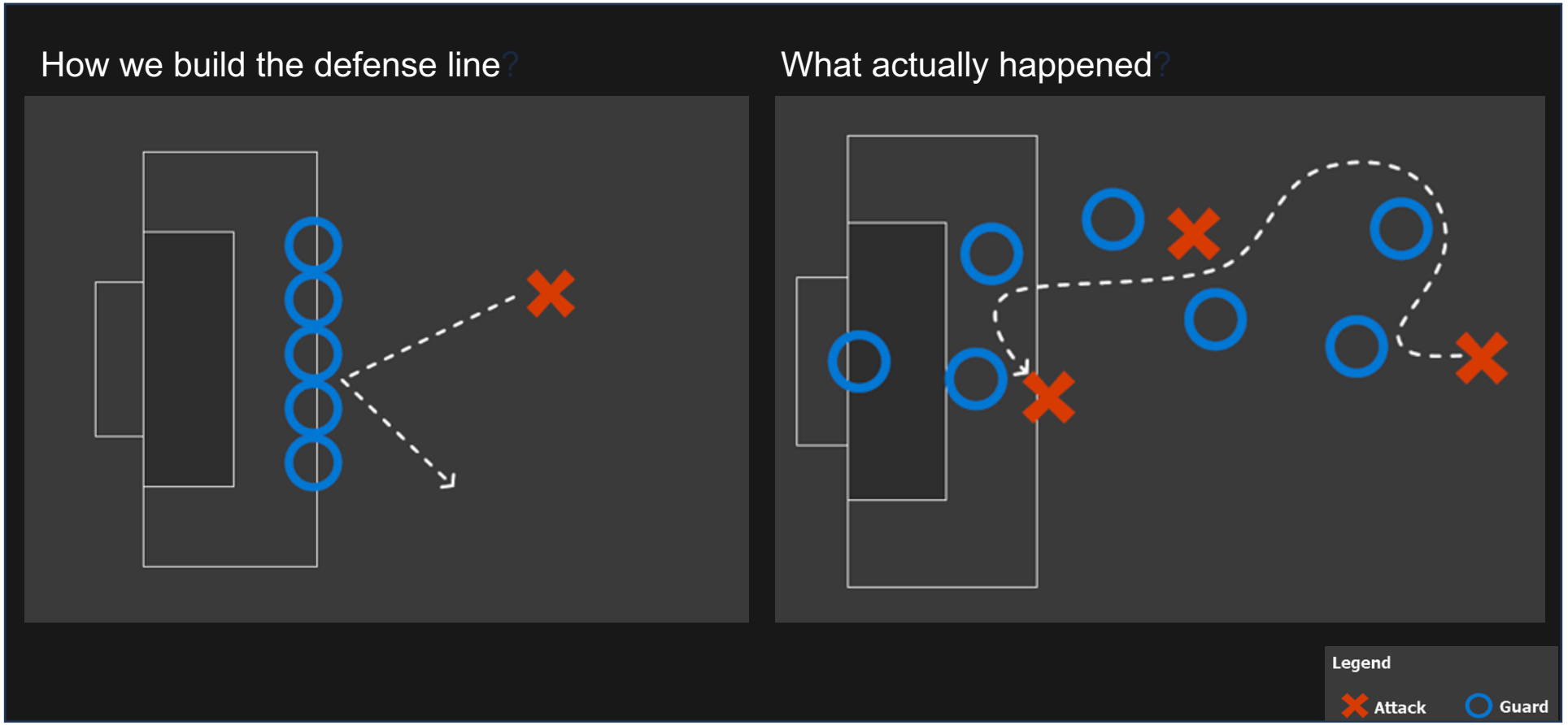
Privacy and security are deeply intertwined

Security control measures are beneficial to privacy, though not enough

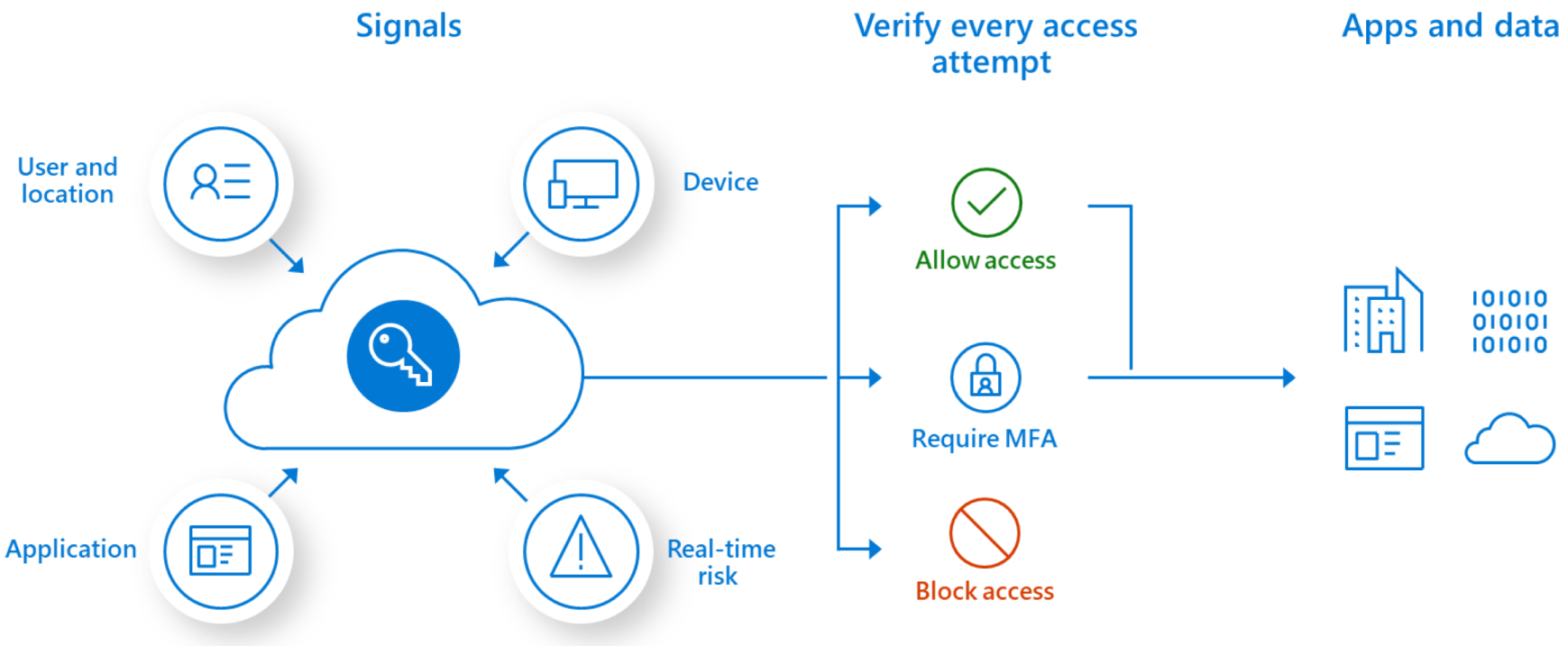
Section 2

Technical Measures for Personal Data Protection

Traditional Security Model

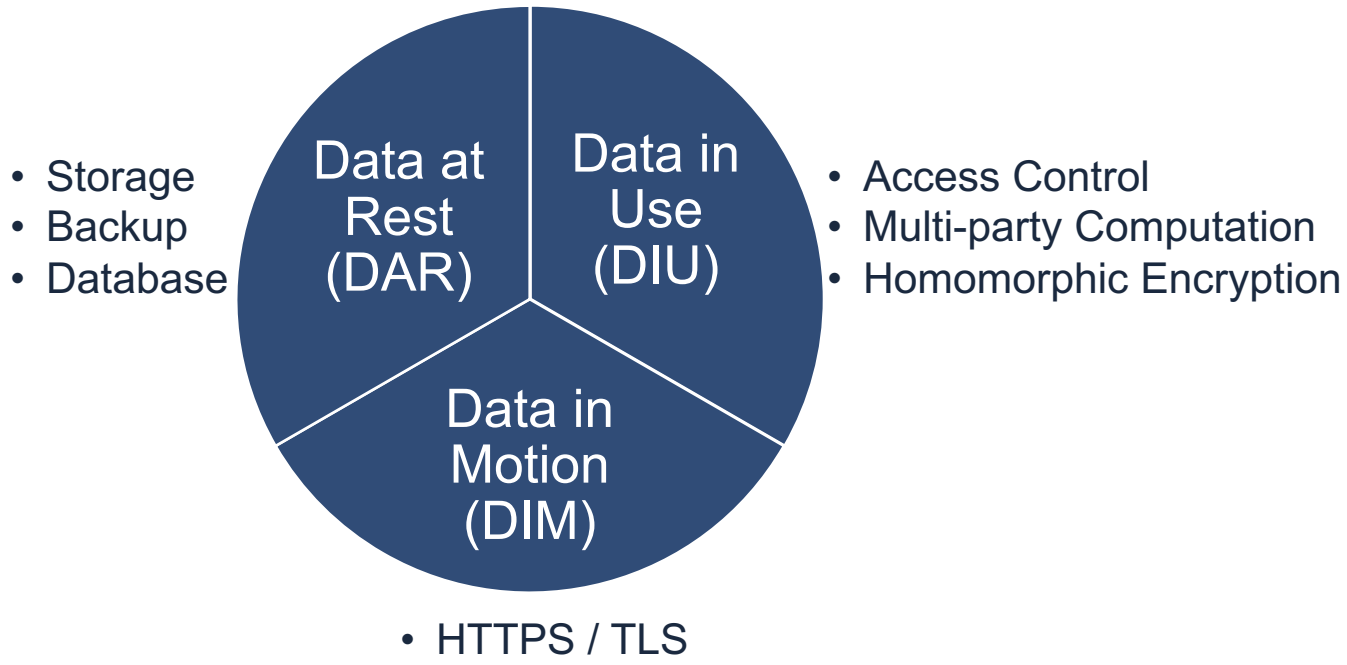


Zero Trust Security Architecture



Common Technical Measures for Protecting Personal Data

- **Encryption**
- **DLP / IRM**
- **IAM**
- **De-identification**



Common Technical Measures for Protecting Personal Data

- **Encryption**
- **DLP / IRM**
- **IAM**
- **De-identification**

Data Loss Prevention

- Prevent data leak out
- Classification
- Detection
- Enforcement

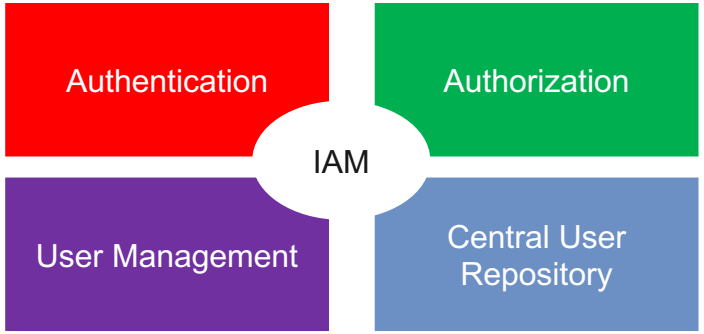
Information Right Management

- Continuous protection wherever document is
- Security control embedded to document

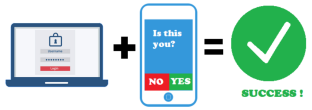
Common Technical Measures for Protecting Personal Data

- Encryption
- DLP / IRM
- IAM
- De-identification

Identity and Access Management



Anti-Phishing



Multi-factor Authentication

Common Technical Measures for Protecting Personal Data

- Encryption
- DLP / IRM
- IAM
- De-identification


ICS 35.040
L 80

GB

中华人民共和国国家标准

GB/T 37964—2019

信息安全技术
个人信息去标识化指南

Information security technology—
Guide for de-identifying personal information

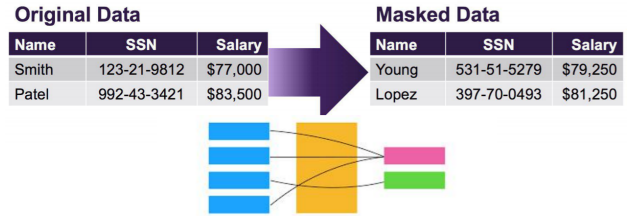
2019-08-30 发布　　2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

- ❑ **Statistical**
  - ✓ Sampling
  - ✓ Aggregation
- ❑ **Suppression**
  - ✓ Masking

440524188*****0014

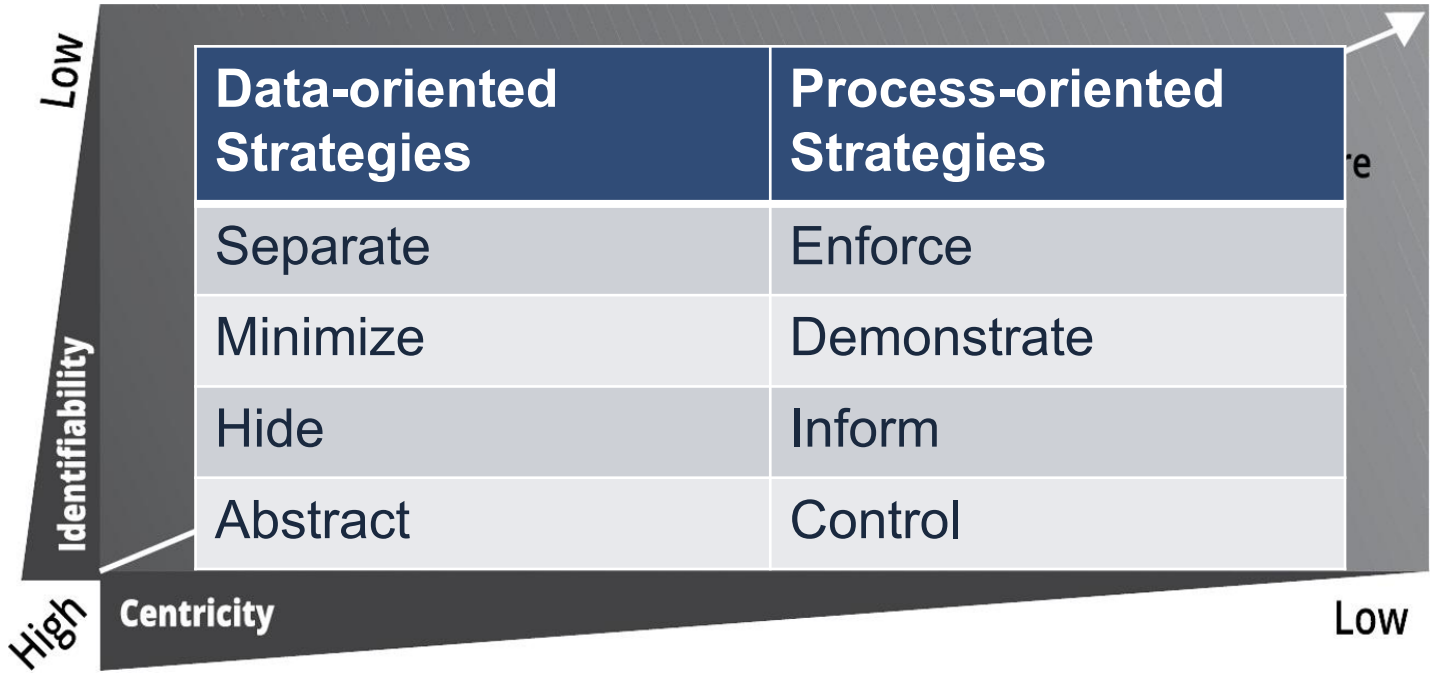
- ❑ **Pseudonymization**



- ❑ **Randomization**
  - ✓ Noise addition

Privacy by Default and by Design

- **Why?**
  - Compliance
  - Cost
  - Assurance
- **Privacy by Default**
  - Least Privilege
  - Opt-in instead of Opt-out
- **Privacy by Design**
  - 7 foundational principles (talk later)
  - 8 strategies

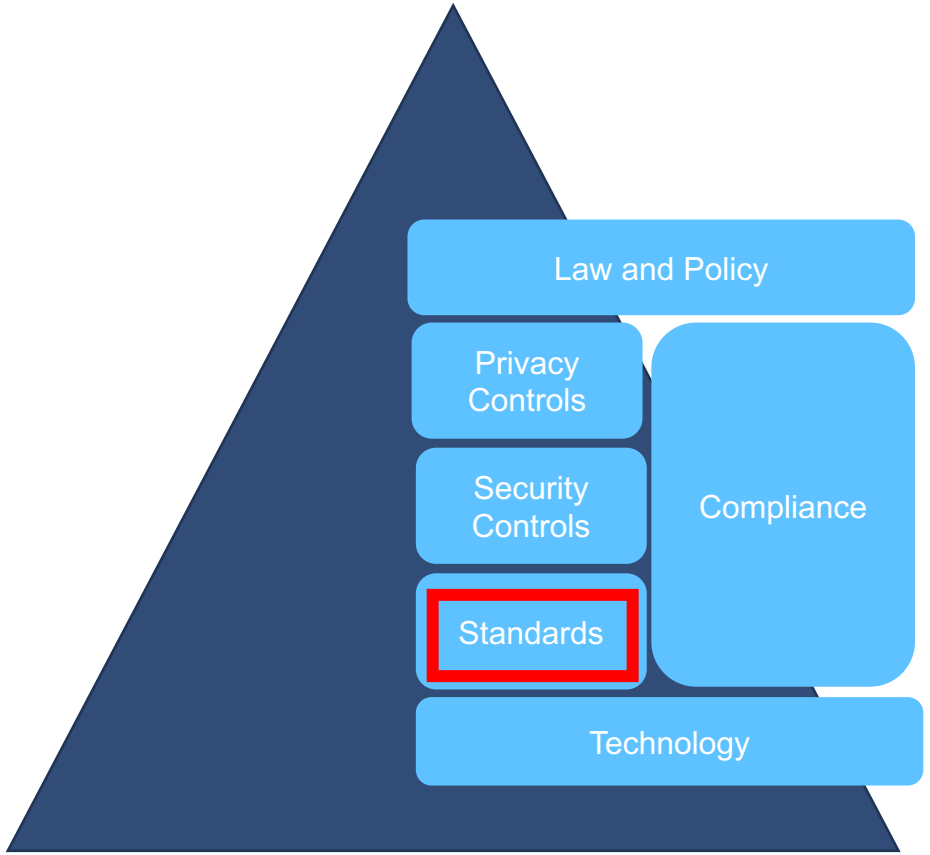


Data-oriented Strategies	Process-oriented Strategies
Separate	Enforce
Minimize	Demonstrate
Hide	Inform
Abstract	Control

Section 3

Organizational Measures for Personal Data Protection

Data Privacy Governance and Engineering



Privacy Governance Program

By Travis D. Breaux

ICS 35.040
L80

中华人民共和国国家标准

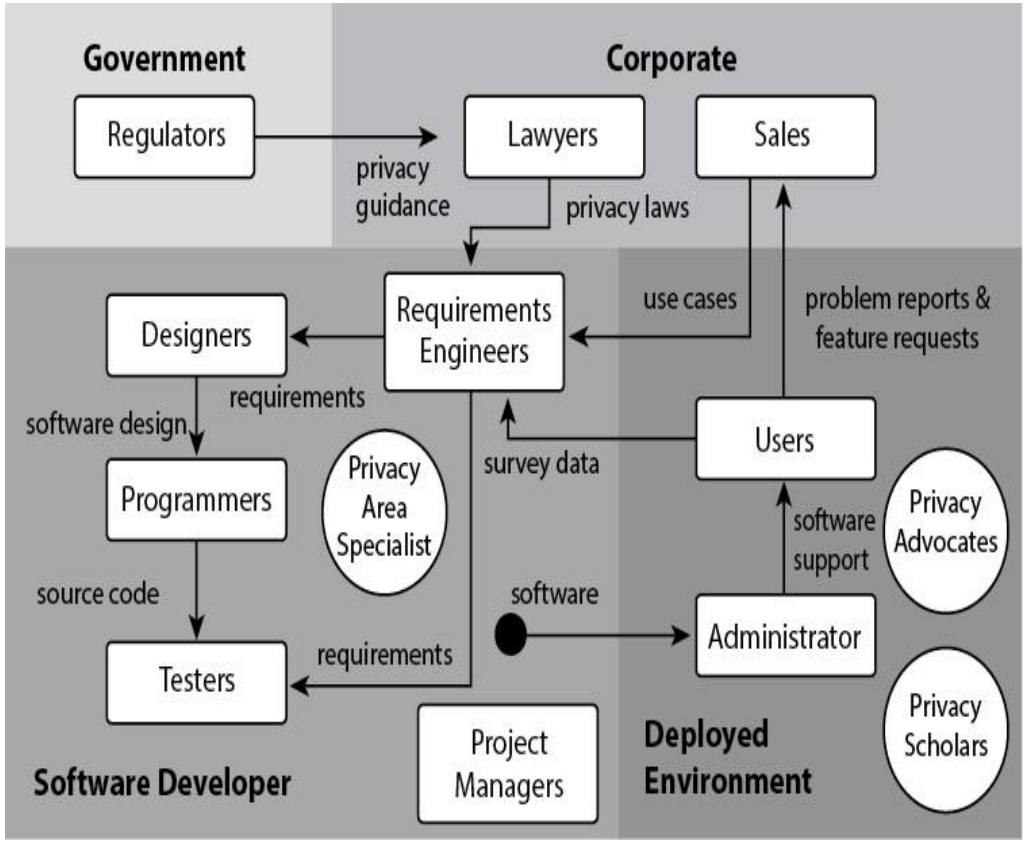
GB/T 35273—2020
代替 GB/T 35273-2017

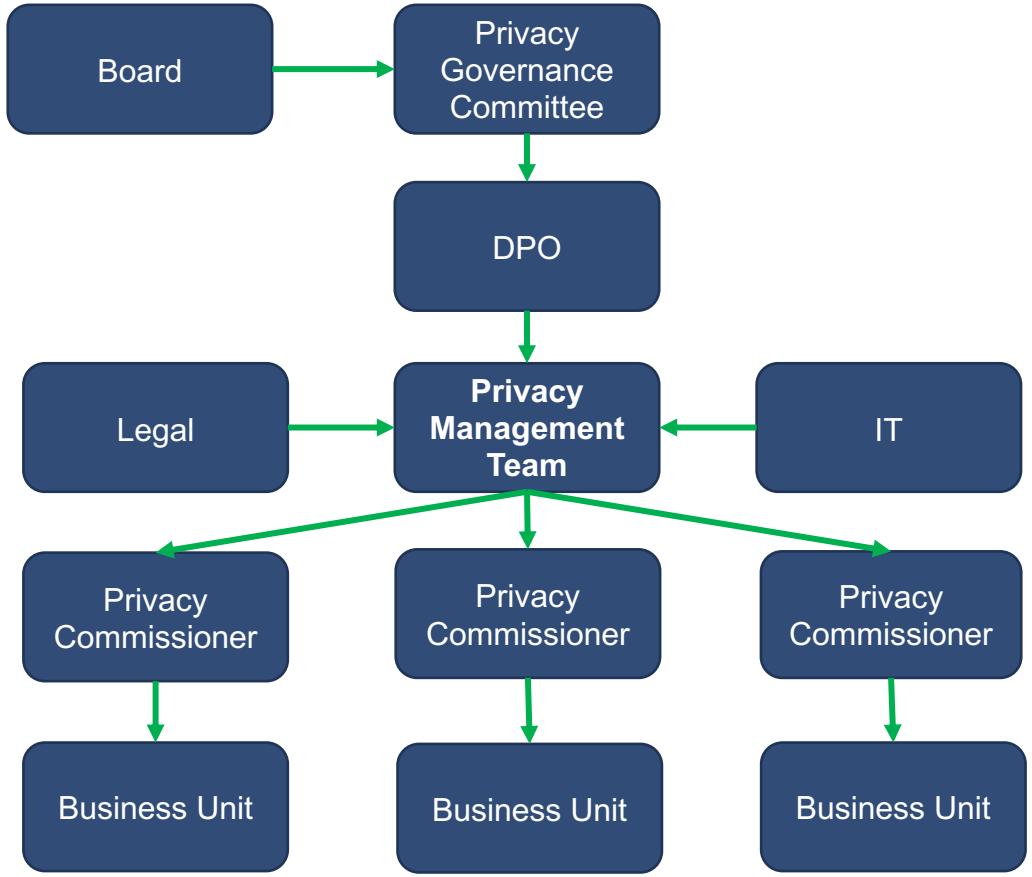
信息安全技术　个人信息安全规范

Information security technology — Personal information security specification

ISO 27001 27701 27018

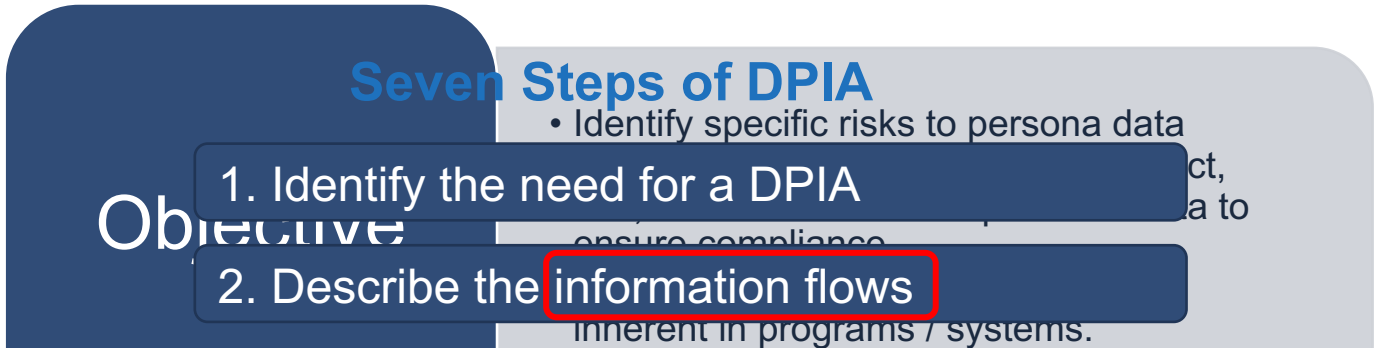
Organization Structure for Privacy Management





DPIA (Data Protection Impact Analysis)

- **What's DPIA?**

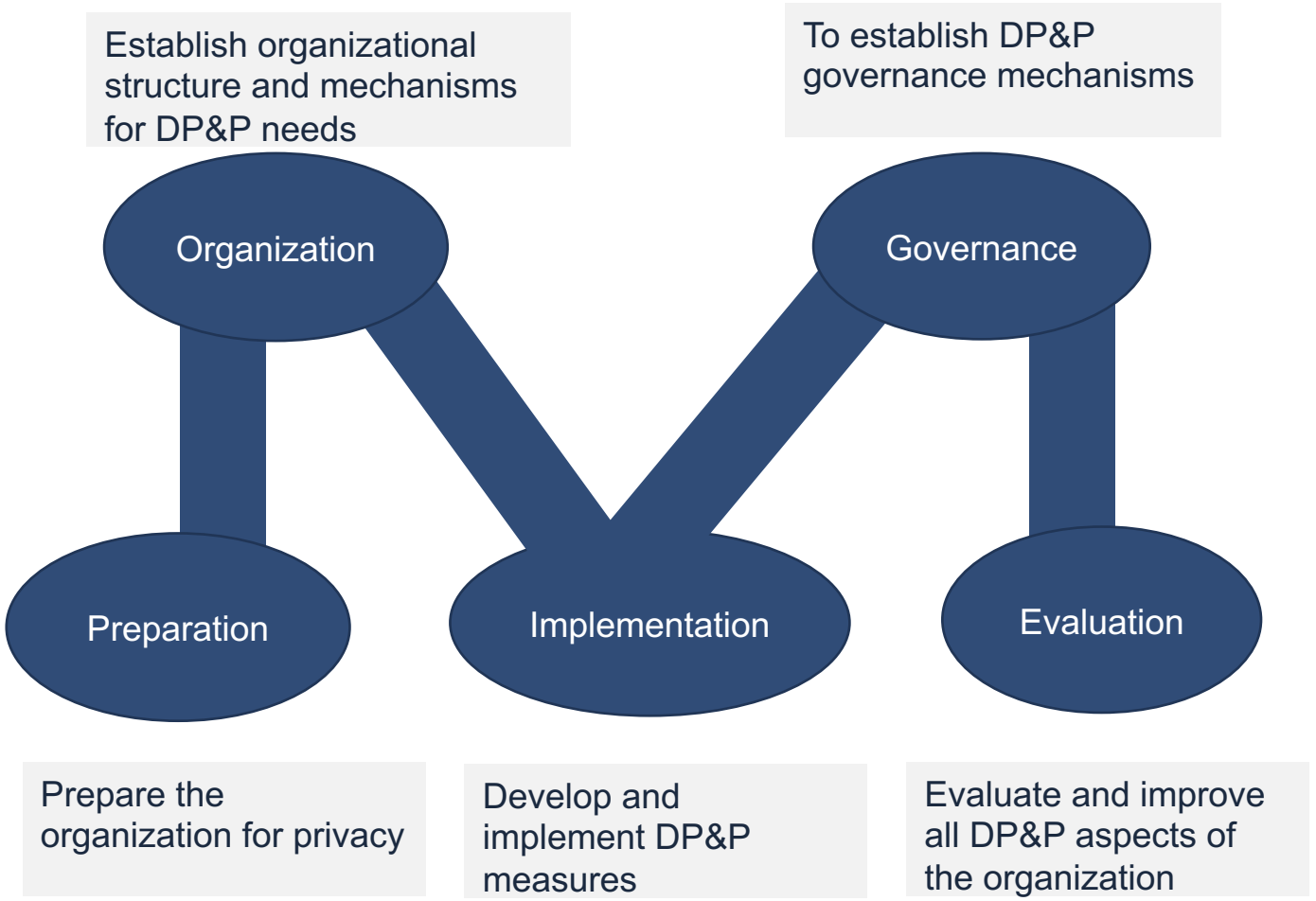


Data Mapping Record Created by:_____ Inputted by:_____ Date:_____ version:_____

Source How was this data collected? >Contact Form >External Orginazation	Personal Data What data are you collecting? >IP Address >Email Address >Phone Number	Reason Why need you collect this data? >CRM >Processing / Analytics	Handling Explain how you will store the data, how it will be processed and who has access to it	Disposal When is the data disposed	consent obtained	subject is over 13	sensitive personal data	Mission critical data
Contact form	Email address Phone number	CRM	Saved to CRM system for marketing event communication, only marketing team needs to access it.	After 6 months	Yes	No	No	Yes

Implementation of DPMS (Data Privacy Management System)

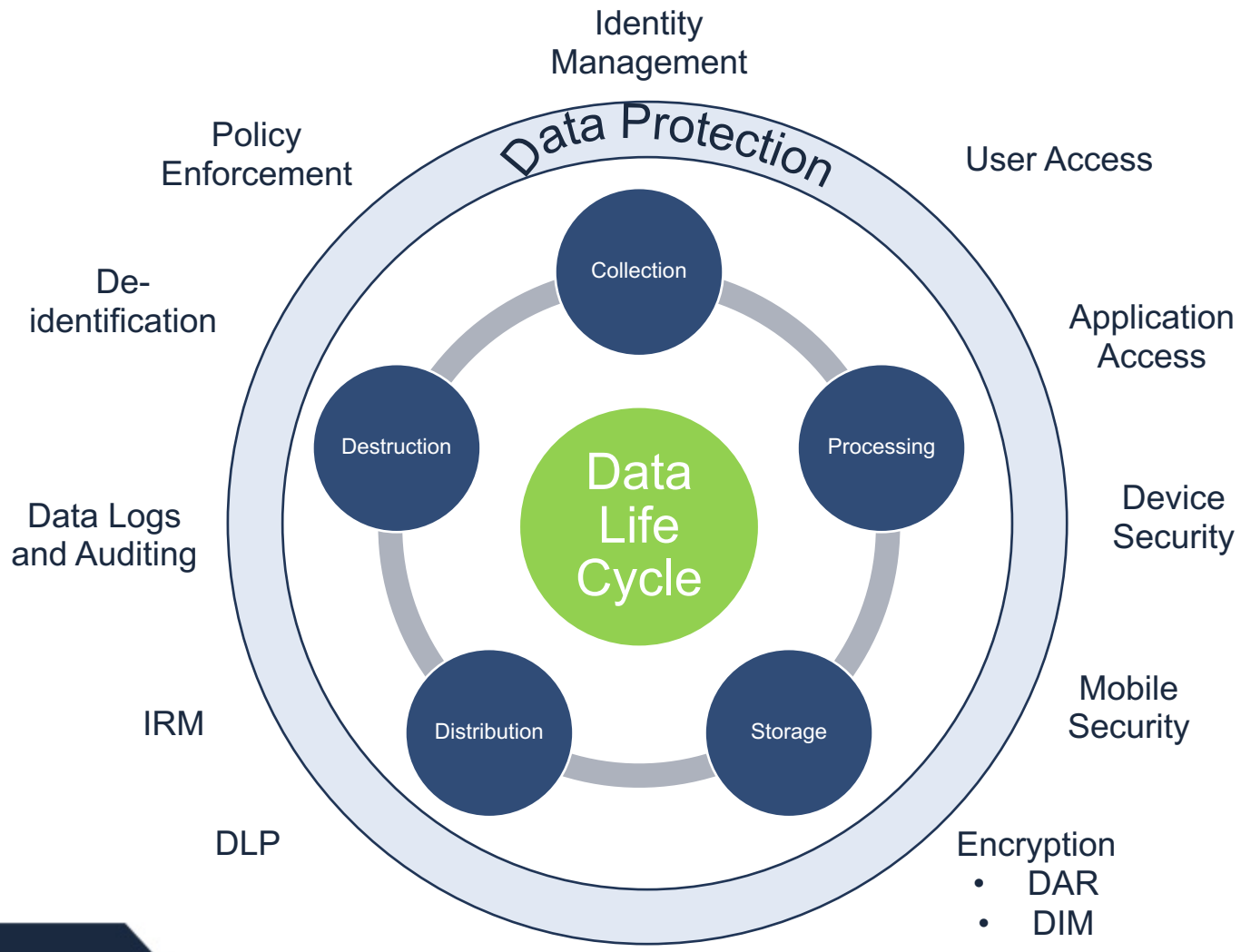
- **DPMS is the combination of Technical and Organizational Measures**
- **The objective of DPMS is design, implement, monitor, assess and improve the Policies, Plans, Procedures, Practices, Controls and Technical Tools.**



Section 4

Overall Consideration / Summary

Overall Consideration of Controls



Seven Fundamental Principles on Privacy -- Ann Cavoukian

1. Proactive, not Reactive; Preventive, not Remedial	Privacy drives the design vs design drives privacy violation
2. Privacy as the Default Setting	Privacy preserving by default / Opt-in vs Opt-out
3. Privacy embedded into Design	Fail to function without privacy-preserving
4. Full functionality: Positive Sum, not Zero Sum	Privacy not a trade-off / win-win solution
5. End-to-End Security: Protection in whole Life Cycle	Every stage: collecting / processing/ storage / distribution, destruction
6. Visibility and Transparency: Keep it Open	Clear and easy to understand privacy notice
7. Respect user's Privacy: Keep it User-centric	Individual as principle beneficiary of privacy and the one affected by privacy violation

DEZAN SHIRA & ASSOCIATES

Your Partner for Growth in Asia

Global Offices

CHINA

Beijing
beijing@dezshira.com

Hangzhou
hangzhou@dezshira.com

Shenzhen
shenzhen@dezshira.com

Dalian
dalian@dezshira.com

Ningbo
ningbo@dezshira.com

Suzhou
suzhou@dezshira.com

Dongguan
dongguan@dezshira.com

Qingdao
qingdao@dezshira.com

Tianjin
tianjin@dezshira.com

Guangzhou
guangzhou@dezshira.com

Shanghai
shanghai@dezshira.com

Zhongshan
zhongshan@dezshira.com

HONG KONG

hongkong@dezshira.com

INDONESIA

indonesia@dezshira.com

SINGAPORE

singapore@dezshira.com

INDIA

Delhi
delhi@dezshira.com

Mumbai
mumbai@dezshira.com

VIETNAM

Hanoi
hanoi@dezshira.com

Ho Chi Minh City
hcmc@dezshira.com

DEZAN SHIRA ASIAN ALLIANCE MEMBERS

Malaysia
malaysia@dezshira.com

The Philippines
philippines@dezshira.com

Thailand
thailand@dezshira.com

DEZAN SHIRA LIAISON OFFICES

Germany
germandesk@dezshira.com

Italy
italiandesk@dezshira.com

United States
usa@dezshira.com

For more information, please visit **www.dezshira.com**

DEZAN SHIRA & ASSOCIATES

Your Partner for Growth in Asia

Scan this QR code

Visit our mobile page and
get the latest updates investors
news and resources with us

Organiser:

BRITISH CHAMBER OF COMMERCE GUANGDONG 广东英国商会

AUSTCHAM SOUTH CHINA
A MEMBER OF AUSTCHAM GREATER CHINA
中国澳大利亚商会-华南

Partner:

中倫律師事務所
ZHONG LUN LAW FIRM

DEZAN SHIRA & ASSOCIATES
Your Partner for Growth in Asia

GZAEFI 广州外商投资企业协会
Guangzhou Association of Enterprises with Foreign Investment

Q & A