

# Canada, EU and China Privacy Law Update

*What US Business Need to Know*

## **Panelists:**

Paige Backman, Partner and Co-chair, Aird Berlis

Christopher Jeffery, Partner and Co-chair, Taylor Wessing

Kate Ying, Partner and Co-chair, Fangda Partners

## **Moderator:**

Roshal Marshall, Managing Chief Counsel, McKesson Corp.

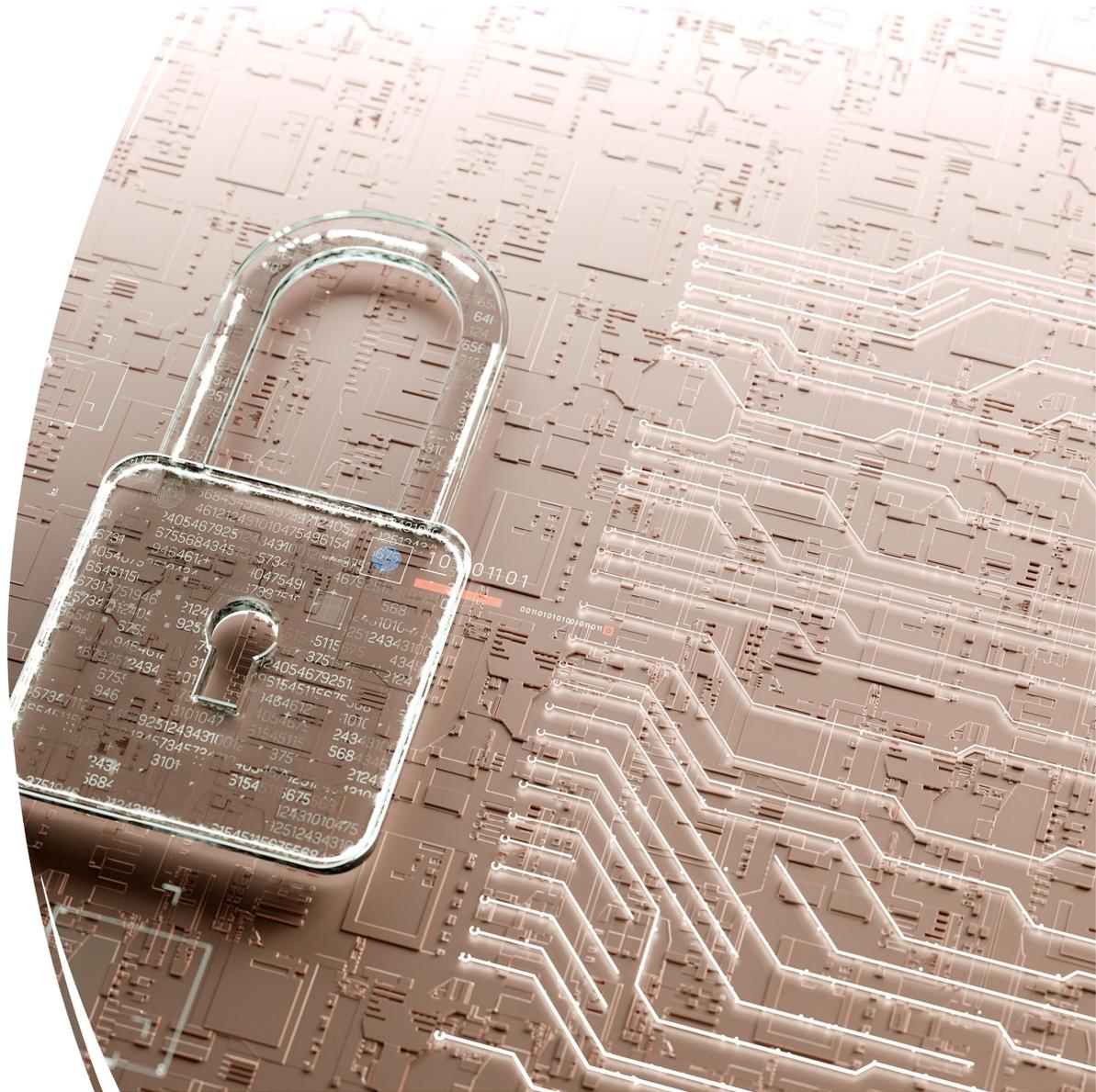
**March 29, 2022**



# Canada Privacy Law Update

---

**Paige Backman,  
Partner, Co-Chair,  
Privacy, Data Security  
Aird Berlis**



## Canada Privacy Law – What U.S. Businesses Need to Know

---

- **Comprehensive- Federal and Provincial legislation**
  - **Private sector, public sector (much broader than the US), health sector**
- **Quasi Constitutional Right (elevated status)**
- **Significant and material changes to privacy laws in Canada pending**
  - **Compliance with EU, but with additional considerations and significant financial penalties**

# Canada Privacy Law – What U.S. Businesses Need to Know

---

- **Application Very Broad**
  - **No minimal threshold for application**
  - **All businesses that process personal information for commercial purposes**
  - **Employment information for federal entities and some provinces**
- **Notices and privacy policies are important, but consent remains key**
- **Data residency and Cross-border Transfers**
  - **Transborder data flow generally permitted with notice.**
  - **Public sector (including education, health) PI in provinces of BC and NS NO transborder transfers or access without consent (subject to limited exemptions)**
  - **Need to assure adequate security including legislative environment**
  - **Transfers and disclosures to any third party (even affiliate) require data processing agreement**
- **Data minimization and reasonableness (can't just collect/use whatever you want, even with notice)**
- **Breach reporting – A reportable breach does not have to involve specific data elements**

# Canada Privacy Law – What U.S. Businesses Need to Know

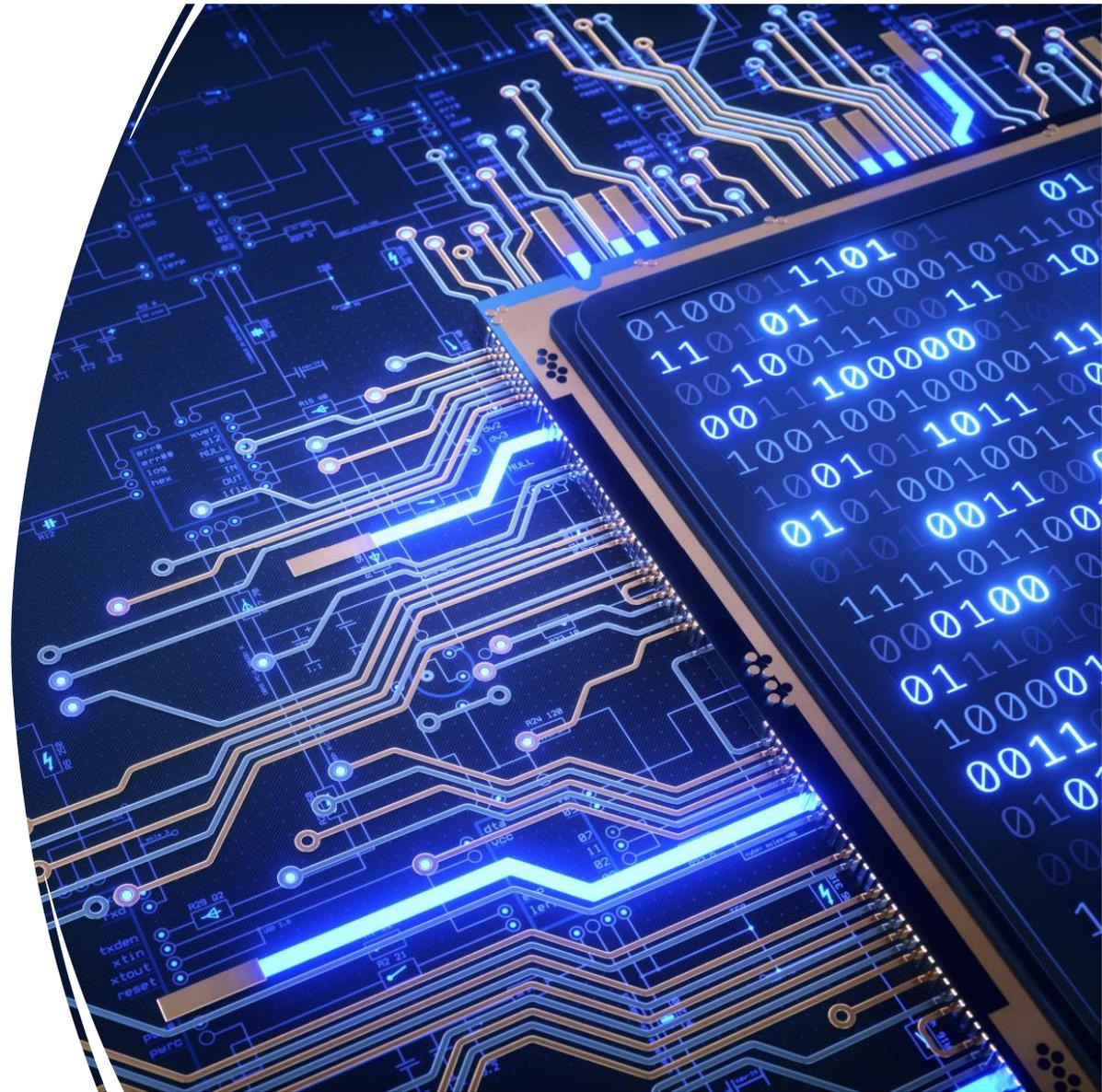
---

- **Significant changes**
- **Quebec leading, federal introduced new law, other provinces bringing new laws into effect**
  - **Privacy Officer (Quebec defaults to CEO unless delegated)**
  - **Mandatory PIAs**
    - **All projects that include PI**
    - **Transfer of PI outside Canada (and outside Quebec when PI is on Quebec residents)**
  - **Additional due diligence on transborder data flow**
  - **AI and Automated decision making**
    - **Additional disclosure obligations, may require human review**
  - **Individual rights strengthened such as right to be forgotten**
  - **Penalties up to 4% global turnover, with potential for doubling**

# GDPR Update

---

**Christopher Jeffrey**  
Partner and Co-Chair  
International US Group  
**Taylor Wessing LLP**



## GDPR - overview

- Active enforcement in Europe – including fines up to 4% of global revenue
- National regional regulators vary in aggression levels – Germany!
- GDPR detailed and complex compliance challenge for them – e.g.
  - Comprehensive data audit and records of all processing
  - Lawful basis to have personal data in the first place
  - Requirements when engaging/contracting with data processors:
    - Diligence, documentation, data transfer, ongoing audit
    - Market moving away from formalistic check the box to deeper dive
  - Data subject rights actually exercised – need vendors to help comply
  - Data transfer assessments & Schrems
  - Direct marketing
  - DPO appointment
  - Security Personal data breach notification
  - Policies, training and implementation – to do GDPR properly a mountain of process and documentation



# How do US B2B companies prioritise?

- For B2B companies, key audience is your customers – with investors and regulators often second (still important)
- Important to see how your platform/ services uses data through the client's eyes
- Key early prioritisation steps aim to create comfort factor and trust and avoid privacy-driven friction in the sales process
- Common early customer-facing deliverables:
  - 'talk the talk' – ensure customer-facing teams have a working knowledge
  - DPA (and flow-down onto your vendors)
  - privacy FAQs/ white papers – comfort that you have thought this through, are on it
- Getting harder and harder to wing it – recommend 2-3 months minimum to prepare just to have the basics in place
- Further governance as you grow



**Taylor Wessing LLP**

# How do US B2C companies prioritise?

- For B2C companies, key audience is consumers, consumer groups and to an extent regulators (they are complaints-driven)
- Key early prioritisation steps aim at "perimeter compliance":
  - Privacy policy, user consent/ sign-up flows
  - Cookie banners
  - Process for data subject rights
  - Direct marketing optin/ optout
- Grow into the rest of GDPR as your European business matures
- In UK, notify the regulator
- Don't buy the "harmonised rules across Europe" spiel

## Hot issue – data transfer

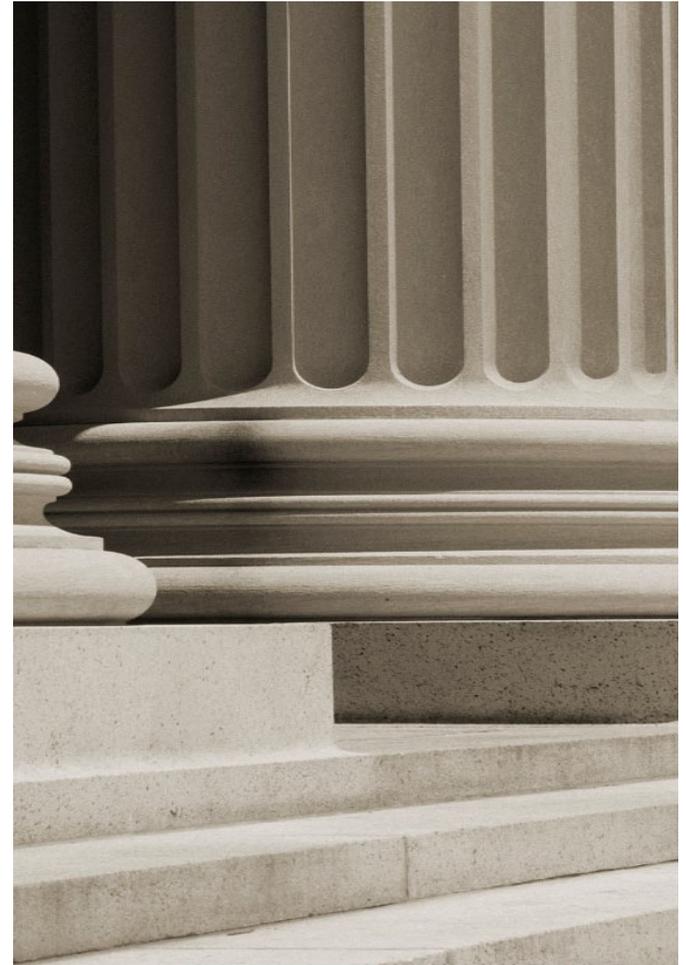
- > General prohibition on personal data transfers outside the UK/ EEA – and a key sensitivity for European clients
- > Schrems judgment and EDPB guidance on assessments to be done, and now new SCCs
  - Some vendors are losing business solely on Schrems concerns
  - A minority of customers scared of using US vendors at all
- > Hard, usually impossible for US companies to silo data in EU, so most use:
  - Model clauses aka standard contractual clauses, and
  - Have key messages straight on where customer data is processed and hosted and how you get customer compliant
  - Recommended: documentation that helps customer with transfer impact assessment under Schrems
  - Sensitivities vary – most acute in regulated sectors, multinationals and Germany, Spain, Poland
- > Binding Corporate Rules the gold standard, but a lot of work



**Taylor Wessing LLP**

# Google Analytics decision

- Austrian regulator: Google Analytics illegal under GDPR:
  - User analytics data transferred to Google US servers
  - Standard contractual clauses in place
  - Google's detailed supplementary measures not enough
  - Only full encryption and keys managed in Europe would have been OK
- Decision supported by French, Dutch and other regulators
- Technical, conservative, disappointing decision
- Under appeal, but question-mark over transfers to US
- Net effect of this - high temperature around data transfer has customers of B2B vendors spooked when dealing with non-European vendors and asking lots of questions
- Offer EU hosting even if transfers for support etc
- In practice transfers continue



**Taylor Wessing LLP**

# China Privacy Law Update

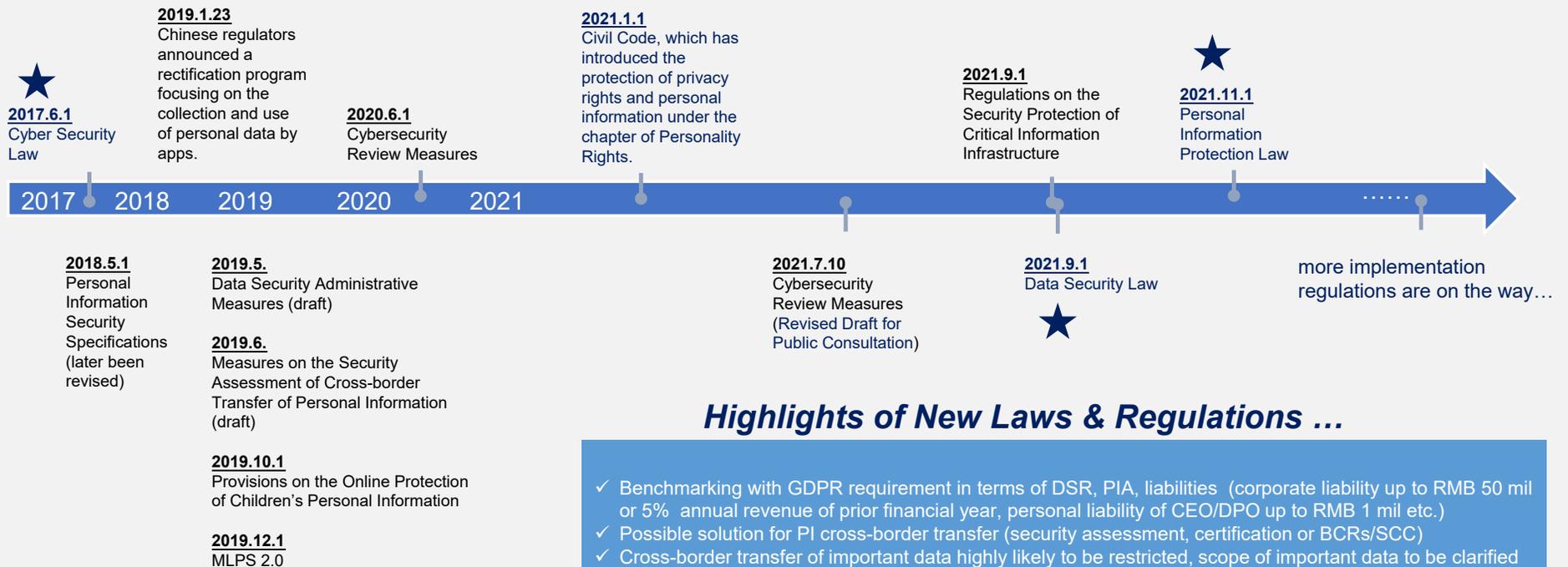
---

Kate Yin, Partner and Co-Chair  
Fangda Law

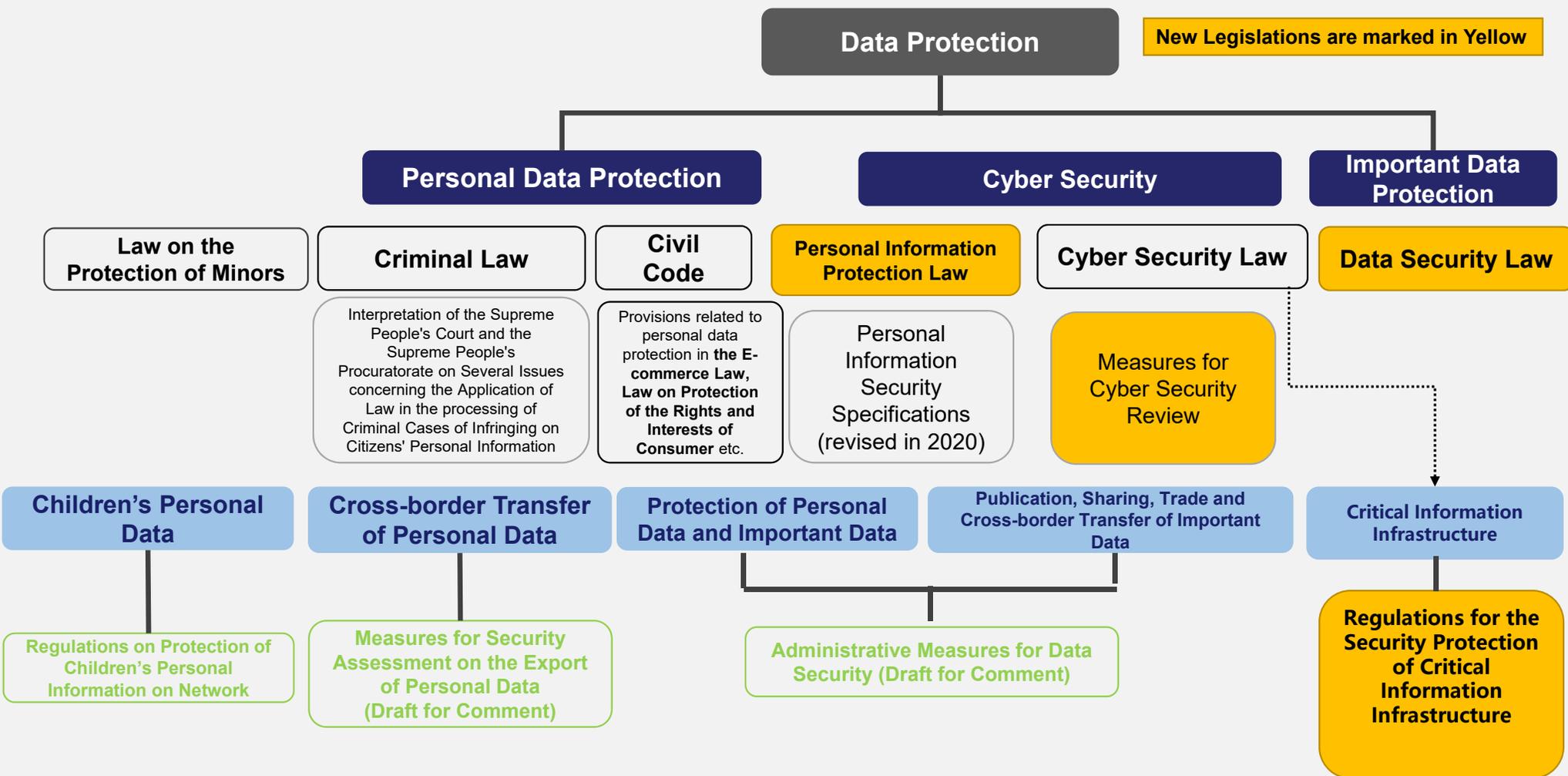


# China's Data Protection Regime Takes Shape

The Data Security Law (“DSL”) and the Personal Information Protection Law (“PIPL”) have been promulgated in 2021. The DSL has become effective from Sep. 1, 2021 and the PIPL will become effective from Nov. 1, 2021. The DSL, the PIPL and the Cyber Security Law (“CSL”) form the foundation of China's data protection regime.



# Overview of Chinese Data Protection Legislation



# Data Security Law (DSL)

## Protection of Important Data and Core Data

1. Establish a data classification and grading protection system and issue the important data directory (potentially on national, local, departmental and industrial level).
2. Introduce the concept of Core Data, with stricter management mechanism and penalties for violation
3. Conduct risk assessment periodically and submit to the competent authorities.

## Regulatory Authorities

1. **Sectorial regulatory authorities** of the industry, telecommunication, nature resources, health, education, defense technology and finance sectors.
2. Public security authorities, state security authorities.
3. State cyber security departments.

## Data Security Review System

1. Conduct **state security reviews** on data activities that impact or may impact the state security.
2. Security review decisions made according to the laws are the **final decision**.

## Countermeasures

If any country or region adopts discriminatory bans, restrictions or other similar measures against China in respect of data-related investment and trade, China may take corresponding measures against such country or region according to the actual situation.

## Data Request

1. **Within China:** where public security authorities or state security authorities need to access data for the maintenance of state security or investigation of crimes, the authorities shall complete **strict approval procedure** and the relevant individuals or organizations shall cooperate.
2. **Outside China:** where foreign judicial or law enforcement authorities request to access data stored within China, such information shall **not be provided in the absence of pre-approval from PRC authorities**. There are penalties for violation of providing data to foreign authorities.

# Important Data Categorization

- “Important data” is a special category of data protected under Chinese laws.
- There is no standardized process to identify important data under Chinese laws and this requires careful assessment of various legal factors to identify the scope of important data.
- Fangda is the only law firm who participates in the drafting of the national standard of important data categorization.

信息安全技术 重要数据识别指南

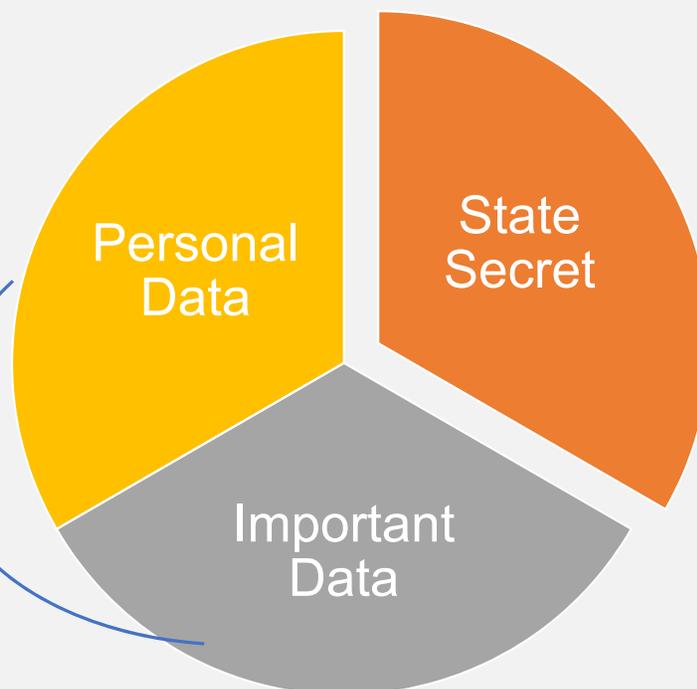
Information security technology - Identification guide of key data

(征求意见稿)

(本稿完成日期: 2021-09-23)

How personal data correlates to important data:

1. Scale
2. Granularity
3. Amount
4. Time
5. Other factors



- Important data refers to non-public data or confidential information that is not state secret but would impact or endanger national interest or public interest of China or impact or endanger society as a whole in China if such non-public data or confidential information is leaked, lost, destroyed, or stolen, modified, access or otherwise illegally processed.
- Given the importance and potential impact of important data to the state security of China, protection of important data is on the regulator's priority.

# Pre-approval on Data Provision to Foreign Authorities and Judicial Bodies

Analysis on pre-approval on data provision to foreign authorities and judicial bodies	Interpretation	Foreign Authorities and Judicial Bodies	The term doesn't include authorities in Hong Kong, nor arbitration tribunals. Semi-government authority share information with foreign governments, and may be viewed as extended bodies of the regulators.
		Authorities	In terms of the purpose of this provision to limit data disclosure to foreign government and prevent harm, it may not be strictly limited to cases of official government enforcements
	Implication	Article 41 of PIPL & Article 36 of DSL may impact on the internal investigation process within your Company, the data provision to foreign courts in litigation, as well as responding to the law enforcements and investigation by foreign authorities (e.g. investigation initiated by SEC or DOJ in the US).	

# Comparison with GDPR and CCPA

Compliance Requirements	Personal Information Protection Law	GDPR	CCPA/CPRA
Accountability	√	√	√
Transparency	√ (More concrete requirements on consent)	√	√
Lawfulness	√ (legal bases like consent, conclusion or performance of contract, statutory obligation, <b>human resource management</b> etc. )	√ (One of the six legal basis like consent and legitimate interests)	√
Sensitive personal data	√	√	√
Purpose limitation	√	√	√
Data minimization	√	√	√
Limited Retention	√	√	√
Manage processing	√ (Agreement and supervision)	√	√
Joint processing	√ (Agreement and joint ability)	√	√
Data localization	√ (CIIO and some personal information processors)	× (Restrictions under Member States' industrial rules)	√
Cross-border data transfer	√ (Agreement, security assessment, certification, <b>International agreements, and necessary measures for adequate protection</b> )	√ (Different data cross-border transfer mechanisms like SCC, BCRs)	√
Data subject rights	√ (Rights to access, copy, correction, supplement, deletion, restriction of processing, withdraw of consent and <b>right to portability</b> )	√	√
Safeguards	√	√	√
DPO	√ (Some personal information processors)	√	×
Documentation	√ (Some data processing activities)	√	×
DPIA	√ (PIA)	√ (High risk data processing activities)	×
Privacy by design/default	√ (PIA)	√	√
Privacy Audit	√	√	√

# Suggestions on the Improvement of Data Compliance System

## Governance structure and document retention

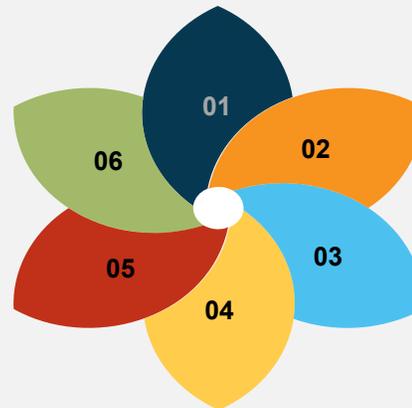
Assigning responsibilities on data protection within the organization, establishing a special department and clarifying the job, and designating a data protection officer if necessary.

## Privacy by design

Privacy by design requires the assessment of products and new business processes or new functions prior to launching them, which could be made with data protection impact assessment (DPIA).

## Compliance with transparency principle

Companies shall inform data subjects on how their personal data are processed and used and their rights.



## Third Parties Management

Managing all third parties or suppliers with which personal data are shared is important to ensure data protection and reduce the liability when third parties have data breach incidents.

## Reactive Measures to data subjects' exercises of data subject rights as well as data breach

Establishing procedures to respond to data subject requests and protect data subject's rights to ensure that the company can notify the regulators within the time limit as well as taking regulation, PR and internal remediation into consideration.

## Cross Border Transfer Scheme

If Company transfers Chinese customers' personal information to a third party abroad, Company should assess the whole process of cross-border data transfer and retain the self-assessment report.

Any Questions?



“Here’s where you give me  
non-comprehending nods of approval.”

[www.shutterstock.com](http://www.shutterstock.com) · 117962926

# Contacts

---



**Kate Yin**

Partner and Co-Chair  
Compliance and Government Enforcement Group  
Fangda Partners  
kate.yin@fangdalaw.com



**Paige Backman**

Partner and Co-Chair  
Privacy & Data Security Group  
Aird & Berlis  
pbackman@airdberlis.com



**Christopher Jeffrey**

Partner and Co-Chair  
International US Group  
Taylor Wessing  
C.Jeffery@taylorwessing.com



## International transfers of personal data

### Use of Google Analytics

#### Recent developments

#### 1. International Transfers

A key element of protecting personal data is making sure that any **international transfers** of data do not result in a loss of privacy and protection for individuals. Transfers of personal data from the UK and the European Economic Area (EEA) to outside countries which are not considered safe (under UK or EU law respectively) are only permissible if an essentially equivalent level of data protection is ensured or if a derogation is available.

Where personal data is transferred to countries that have different laws and data protection compliance requirements, additional protections may be required to ensure those transfers are lawful under EU and UK data protection laws.

As part of this process, where data is collected by a controller or processor in the EEA, organisations usually overcome the restrictions around international data transfers by implementing contracts with international data recipients that reflect the European Commission's latest set of standard contractual clauses as of June 2021. Organisations should also prepare to do the same for data originating in the UK, with the UK Information Commissioner's Office approved set of data transfer clauses set to take effect in March 2022.

For transfers to the US, the 2020 CJEU '**Schrems II**' decision meant that existing export mechanisms in use between the EEA and the US were considered inadequate to ensure protection of personal data (most notably to prevent access by intelligence agencies).

Following this decision, EU-based organisations were required to:

- undertake an assessment of each of its transfers to the US (and to any jurisdiction without an adequacy decision) to decide whether the protection provided to the data is essentially equivalent to the protection provided under EU law; and
- put in place enhanced protections (known as supplementary measures) if needed following that assessment. This includes monitoring any regulatory developments and re-evaluating the transfer at appropriate intervals.

#### 2. Monitoring developments: Use of Google Analytics

##### *The Google Analytics service*

Google Analytics provides a set of tools that supports organisations to measure engagement on their websites (e.g., the type of device or browser used, how long, on average, visitors spend, or roughly where geographically visitors are coming from). In this context, a unique identifier is assigned to each visitor. This identifier (which constitutes personal data, albeit in a very basic form) and any associated data are transferred to Google in the United States.

##### *The privacy challenge to the service*

Privacy campaigners have formally challenged the use of the Google Analytics service (and similar services) in the EU. This campaign has taken the form of a large number of complaints to regulatory bodies across the EU, which focused on the transfer of data collected via the Google Analytics service to Google in the US. The campaigners were particularly concerned about the potential for access by the US intelligence agencies (a key issue in the Schrems II decision).

The challenge has been brought in almost all EU Member States and regulators are now starting to respond. We know that the European Data Protection Board has formed a taskforce to co-ordinate these responses so we expect the position of data protection regulators in various Member States to be consistent.

#### *EU regulatory decisions regarding Google Analytics*

The first decision on this matter was announced by the Austrian Data Protection Authority (DSB) who ruled that the Google Analytics service breaches EU law on data exports. Although the website owner and Google argued to the contrary, the DSB found that the data collected through Google Analytics was personal data and it was transferred to the US where US surveillance laws do not provide an essentially equivalent level of protection of personal data by GDPR standards. The supplementary measures that Google had implemented were not considered sufficient to the DSB. The decision means that Austrian website providers using Google Analytics may be in violation of the GDPR.

In addition, not long after the DSB decision, the French Data Protection Authority (CNIL) also concluded that the Google Analytics service is unlawful – stating, similar to the DSB, that the service does not provide sufficient guarantees to exclude user data from being accessed by US intelligence services. Consequently, the privacy of French website users, whose data is exported by the Google Analytics service to the US, is at risk. French websites must now take steps to bring processing into compliance with the GDPR, if necessary, by ceasing to use the Google Analytics functionality.

The CNIL decision was reached 'in cooperation with its European counterparts'. On this basis we expect similar regulatory decisions to be reached across the EU. The Dutch and Danish Data Protection Authorities have issued holding statements – noting that they are considering the Austrian DPA's decision.

#### *The response from Google*

Google issued a robust [response](#), arguing that there was a fundamental misunderstanding with how Google Analytics works. In particular, underlining that Google Analytics does not track people or profile them across the internet. Rather it helps organisations understand how their services and apps are used. They argue that the data is never used by Google to identify a person. Google also affirmed that in 15 years of providing Google Analytics, it has never received a request for disclosure of data collected by this tool from US intelligence bodies.

So where does this leave us?

### **3. What should website operators do now?**

Clearly, there are question marks hanging over the continued general use of the Google Analytics service in the EU (so far, the UK's regulator – the Information Commissioner's Office – has not published a statement on their position). However, Google's response shows that they are prepared to challenge the current Austrian and CNIL regulatory positions. Whichever

way the issue progresses, the onus will fall on website owners to determine an organisations' continued compliance.

The following protections are likely to be the most useful steps that website owners can take whilst they consider their use of Google Analytics going forwards. These should be implemented, documented and form part of an organisation's compliance strategy whilst we await additional outcomes from EU regulators or from Google itself:

- **control whether Google is permitted to use analytics data for its own further specified purposes** (such as technical support or to improve its products and services). If you have opted into such services you may now wish to specifically opt-out to retain control over uses of the data.
- **take advantage of Google Analytics privacy controls and resources.** Google will act on the instructions of website owners. Consider applying additional controls where permitted by the service, including ensuring IP anonymisation (although be aware that the regulator may not consider this feature as implementing true anonymisation), disabling data collection on certain web-pages, and setting sensible retention periods for Google Analytics data based on necessity.
- If, as part of your review, you recognise that unnecessary personal data has been uploaded to the Google Analytics service (e.g. full IP addresses), then website owners can **make use of Google Analytics deletion tools** for this personal data to ensure it is scrubbed from the service.
- **Carry out a documented review of Google's own security measures.** Google uses a number of supplementary measures in addition to the usual standard contractual clauses for data transfers. These include anonymising IP addresses before data leaves Europe, using data encryption, technical measures to prevent interception, and international security standards (such as ISO 27001). We recommend IT and security teams familiarise themselves with Google's security measures, record this as a documented review, and note any internal comments on the adequacy of those measures for your specific website's data flows.
- **Flag to website users the availability of protective controls.** Most websites will already reference in a privacy or cookies policy the fact that Google Analytics is in operation. Website owners should consider a more prominent flag on its website for its use of the Google Analytics service, with specific instructions to users on the availability of disabling Google Analytics using the Google-provided add-on.

As a final option, website owners could **cease using Google Analytics altogether**, or **find an EU-based alternative** that does not suffer the same issues with international transfers. We would recommend, however, taking the initial protective steps above as a primary option, and waiting to see any further EU regulatory responses (including a central EU opinion) before taking any more definitive steps.

March 2022

Ed Hadcock, [e.hadcock@taylorwessing.com](mailto:e.hadcock@taylorwessing.com)

Chris Jeffery, [c.jeffery@taylorwessing.com](mailto:c.jeffery@taylorwessing.com)

**Taylor Wessing LLP**