MAYER | BROWN

Cyber Spotlight: *Cybersecurity Developments in Europe, the UK and China*

National Cybersecurity Awareness Month
Do your part. #BeCyberSmart

Today's Speakers

Gabriela Kennedy
Partner, Hong Kong
+852 2843 2380
gabriela.kennedy@
mayerbrown.com

Ana Hadnes Bruder
Senior Associate, Frankfurt
+49 69 7941 1778
abruder@mayerbrown.com

Oliver Yaros
Partner
+ 44 20 3130 3698
oyaros@mayerbrown.com

Today's Agenda

- The implications for businesses seeking to comply with China's new Data Security Law and Personal Information Protection Law in combination with the existing Cybersecurity Law requirements.
- Latest developments relating to the EU Cybersecurity Act and the European Union Agency for Cybersecurity's (ENISA's) cybersecurity assessment methodology.
- Transferring personal data from Europe under the new, finalized European Standard Contractual Clauses and European Data Protection Board (EDPB) Recommendations and the practical challenges they pose.
- Cybersecurity and data privacy developments in the UK and the implications for businesses in a post-Brexit world.
- Questions?

Developments in China

MAYER | BROWN

Cybersecurity Law

Generally regulates network and data security (with some provisions regulating data privacy)

Provides a high level framework regulating the collection, storage, transmission and use of electronic data (with additional piecemeal guidelines issued since CSL came into force in 2017)

Covers all network operators and critical information infrastructure (CII) operators

Cybersecurity

- Requirement to carry out security assessment under Multi-Level Protection Scheme (MLPS)
- Certification requirements relating to procurement of critical cybersecurity equipment and products
- Data localization and cross-border transfer restrictions for important data (for CII operators)
- Cyber incident notification requirements
- Additional security requirements imposed on CII operators

Data Privacy

- Requirements relating to collection, storage, transmission and use of personal information
- Consent requirements
- Data localization and cross-border transfer restrictions for personal information (for CII operators)
- Grants individual rights (e.g. right to correction and erasure)

Data Security Law

Came into force on 1 September 2021

Regulates the processing of any data	• Defined as any record of information in electronic or non-electronic format • Includes non-personal data and "important data" • Introduces new category of "national core data"
Expands the scope of certain obligations of network and CII operators under the CSL	• Must establish a data security management system based on the multi-level protection scheme • Carry out data security training • Implement technical security and safeguarding measures • Carry out regular risk assessments on the processing of "important data" • Restrictions on handling data requests by foreign judicial or law enforcement organs
Expands scope of restrictions on cross-border transfers of "important data" to non-CII operators	• Echoes the stricter requirements under the Draft Measures on Security Assessment of the Cross-Border Transfer of Personal Information ("**2019 Draft Measures**") issued under the CSL • 2019 Draft Measures expected to be further amended to align with Data Security Law and draft Personal Information Protection Law

Personal Information Protection Law

To take effect on 1 November 2021

China's first comprehensive law that protects personal information

- Has extra-territorial effect
- Sets out rules for collecting and processing personal information (e.g. consent requirements and other legal bases for processing), rights of data subjects, obligations of data processors, liabilities for breach (e.g. revenue-based penalties, revocation of business licence), etc.
- Data localisation requirements for CII operators or entities processing personal information above a specified volume

Imposes additional requirements on cross-border transfers of personal information for all entities

Fulfill at least one requirement:

- Entering into an agreement with the foreign recipient based on "standard contract" to be specified by the Cyberspace Administration of China (CAC)
- Certified by a specialized agency according to CAC's requirements
- Pass security assessment by government authorities (mandatory if transferor is a CII operator or an entity that processes personal information above a specified volume)

Key Data Privacy Laws in the PRC

	Cybersecurity Law (effective since 1 June 2017)	Data Security Law (effective since 1 June 2017)	Personal Information Protection Law (effective since 1 June 2017)
Purpose of regulation	Provide general data protection and cybersecurity obligations	Contains detailed data security-specific obligations	Contains detailed data privacy-specific obligations
Type of entities covered	Covers all network and CII operators	Covers all entities carrying out data processing activities within the PRC	Covers all entities handling personal information of individuals within the PRC
Type of data covered	All types of data (electronic only)	All types of data (both electronic and non-electronic), with additional focus on "important data" and "national core data"	Personal information only

Takeaway Points/Compliance Steps

Consider applicability and risks of the various PRC privacy/cyber laws	• Note the extra-territorial effect (e.g. PIPL) • Potentially severe penalties (e.g. revenue-based fines, revocation of business licence, etc.)
General compliance gap analysis	• Data mapping ("regular" data, personal data (sensitive vs non-sensitive), important data) • Assess existing data collection, use, storage, disclosure, security practices in light of relevant obligations and implement remedial measures to plug gaps
Multi-level protection scheme	• Engage expert to assess classification level in relation to MLPS • Classification level will affect relevant data and network security obligations
Data localisation and cross-border transfers	• Minimise data transferred into / collected in the PRC • Store all PRC data on local PRC servers / segregation of data and systems • Comply with cross-border transfer requirements (e.g. conduct security assessment, obtain authorities' approval)
Restrictions on data access by foreign authorities	• Consider storing such data outside of the PRC instead to avoid any complications in future when seeking to fulfil such requests from such foreign authorities

Developments in the EU

EU Cybersecurity Act (Regulation (EU) 2019/881)

- The Cybersecurity Act (CSA) establishes a cybersecurity certification framework for products and services and provides a permanent mandate to the EU Agency for Cybersecurity (ENISA)
- Came into force on 27 June 2019 and applies in full as of 28 June 2021
- Legal basis for EU-wide cybersecurity certification framework for Information and Communications Technology (ICT) products, services and processes
- Strengthens ENISA:
  - More resources and new tasks, such as:
    - Setting up and maintaining European cybersecurity certification framework
    - Informing the public on the certification schemes

ENISA Methodology for a Sectoral Cybersecurity Assessment

- Published on 13 September 2021
- Addressed to an **expert level audience**
- Content:
  - Objectives in the context of ICT security for sectoral multi-stakeholder systems,
  - Drafting sectoral cybersecurity certification schemes.

- Goal: **Increasing trust** in ICT services and products through cybersecurity certification
  - Cybersecurity certification schemes must be well accepted by the market

ENISA Methodology for a Sectoral Cybersecurity Assessment

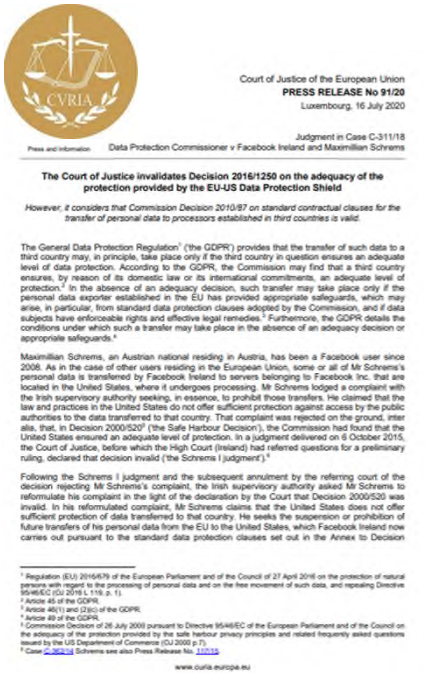
- Basic principle: establishment of a sound **understanding** of the sectoral ICT services and system as a foundation for all other functions:
  - Focus on cybersecurity assessment at the sectoral level
  - Introduces a common, scalable approach to risk-based security and assurance

- Promotion of the **market acceptance** of cybersecurity certification:
  - Supports the identification of risks associated with the intended use of ICT systems
  - Introduces a common concept for security levels.

Schrems II and Standard Contractual Clauses

Major takeaways from *Schrems II* (CJEU case no. C-311/18) decision, issued on July 16, 2020:

- **EU-US Privacy Shield no longer a legal basis for transfers** from the European Economic Area to the USA
- Standard Contractual Clauses ("**SCCs**") continue to be a transfer instrument, *however*:
  - Level of protection in the third country needs to be assessed
  - Appropriate supplementary measures in addition to SCCs might need to be taken



Court of Justice of the European Union
PRESS RELEASE No 91/20
Luxembourg, 16 July 2020

Judgment in Case C-311/18
Data Protection Commissioner v Facebook Ireland and Maximillian Schrems

The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield

However, it considers that Commission Decision 2010/87 on standard contractual clauses for the transfer of personal data to processors established in third countries is valid.

The General Data Protection Regulation[1] ('the GDPR') provides that the transfer of such data to a third country may, in principle, take place only if the third country in question ensures an adequate level of data protection. According to the GDPR, the Commission may find that a third country ensures, by reason of its domestic law or its international commitments, an adequate level of protection.[2] In the absence of an adequacy decision, such transfer may take place only if the personal data exporter established in the EU has provided appropriate safeguards, which may arise, in particular, from standard data protection clauses adopted by the Commission, and if data subjects have enforceable rights and effective legal remedies.[3] Furthermore, the GDPR details the conditions under which such a transfer may take place in the absence of an adequacy decision or appropriate safeguards.[4]

Maximillian Schrems, an Austrian national residing in Austria, has been a Facebook user since 2008. As in the case of other users residing in the European Union, some or all of Mr Schrems's personal data is transferred by Facebook Ireland to servers belonging to Facebook Inc. that are located in the United States, where it undergoes processing. Mr Schrems lodged a complaint with the Irish supervisory authority seeking, in essence, to prohibit those transfers. He claimed that the law and practices in the United States do not offer sufficient protection against access by the public authorities to the data transferred to that country. That complaint was rejected on the ground, inter alia, that, in Decision 2000/520[5] ('the Safe Harbour Decision'), the Commission had found that the United States ensured an adequate level of protection. In a judgment delivered on 6 October 2015, the Court of Justice, before which the High Court (Ireland) had referred questions for a preliminary ruling, declared that decision invalid ('the Schrems I judgment').[6]

Following the Schrems I judgment and the subsequent annulment by the referring court of the decision rejecting Mr Schrems's complaint, the Irish supervisory authority asked Mr Schrems to reformulate his complaint in the light of the declaration by the Court that Decision 2000/520 was invalid. In his reformulated complaint, Mr Schrems claims that the United States does not offer sufficient protection of data transferred to that country. He seeks the suspension or prohibition of future transfers of his personal data from the EU to the United States, which Facebook Ireland now carries out pursuant to the standard data protection clauses set out in the Annex to Decision

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ 2016 L 119, p. 1).
[2] Article 45 of the GDPR.
[3] Article 46(1) and (2)(c) of the GDPR.
[4] Article 49 of the GDPR.
[5] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 p.7).
[6] Case C-362/14 Schrems see also Press Release No. 117/15.

www.curia.europa.eu

Recent Developments: EDPB Guidance

Guidance from European Data Protection Board ("**EDPB**") published on June 21, 2021

- Major takeaways from the EDPB guidance:
  - **Conduct a local law and practices assessment** in the jurisdiction where the data is transferred to ("transfer impact assessment")
  - Where necessary, **implement supplementary measures for such transfers** (e.g., encryption, pseudonymization)
  - If supplementary measures necessary but not possible, the transfer would not be lawful, unless it could be based on Article 49(1) GDPR derogations

New Standard Contractual Clauses (SCCs)

New EU Standard Contractual Clauses for data transfers adopted on 4 June 2021

- The new SCCs:
  - **Replace controller-to-controller and controller-to-processor SCCs** adopted prior to GDPR
  - **Follow a modular approach** (controller-to-processor module obviates need for separate data processing agreements)
  - **Require data exporter and importer to assess the local laws** in the export jurisdiction
  - Require **specific description** of technical and organizational measures adopted
  - **impose obligations on data importer** in case of access by public authorities
- Agreements concluded as of 27 September 2021 need to implement the new SCCs
- Businesses will have until 27 December 2022 to replace old SCCs with new SCCs

Developments in the UK

MAYER | BROWN

The UK position post-Brexit

- Largely still following the position
  - The UK GDPR now applies instead of the EU GDPR
  - UK Security of Network & Information Systems Regulations still implements EU NIS Directive
  - Old EU case law and final guidance still applicable (Schrems II etc)
  - But new EU case law and guidance (e.g. EDPB Recommendations) persuasive only
- BUT change is on the horizon!

UK Developments Post-Brexit

- UK Government announcements include:
  - UK Cyber Security Legislation for Consumer Products
  - Code of Practice for Consumer Internet of things (IoT) Security
  - UK Online Safety Bill
  - Consultation to reform UK Data Protection Law and the UK Information Commissioner's Office / divergence from EU rules
  - Changes to the rules on the transfer of personal data from the UK

Questions?