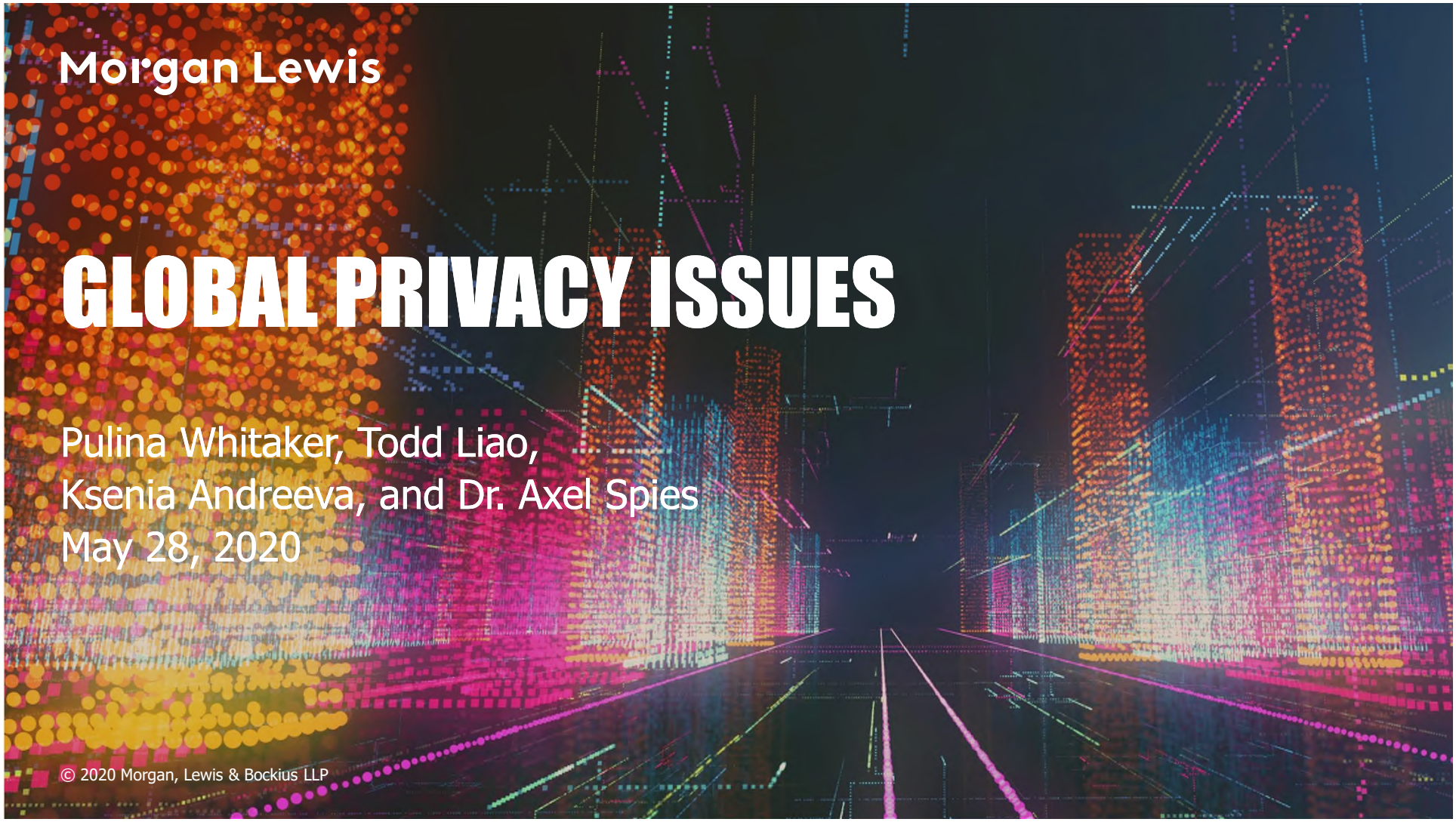

Morgan Lewis
GLOBAL PRIVACY ISSUES
Pulina Whitaker, Todd Liao,
Ksenia Andreeva, and Dr. Axel Spies
May 28, 2020
© 2020 Morgan, Lewis & Bockius LLP

SECTION 01

UK PRIVACY ISSUES AND A DISCUSSION OF BREXIT

UK Data Protection Act 2018

- UK Data Protection Act 2018 – in force on 25 May 2018
- Implements local law permitted provisions of GDPR:
  - children's consent at 13 years;
  - processing for criminal records;
  - exemptions from restrictions for processing special categories of interest e.g. public interest exemptions;
  - exemptions from subject access rights
- Includes law enforcement processing and intelligence services processing provisions
- Sets out powers of enforcement of ICO

Brexit – a new world?

- Unlikely…
- UK GDPR will be implemented to give direct effect to GDPR
- Other data privacy laws already incorporated in UK law e.g. ePrivacy Regulations give effect to Electronic Communications Directive

UK Data Exports

- We will not be "adequate" automatically – need a European Commission determination for data transfers
- Do we apply – could take years
- Likely to depend on a trade deal
- EU-US privacy shield will apply but US companies need to reference UK transfers in privacy policies
- ICO has approved standard contractual clauses – likely to be replaced in future with UK versions

SECTION 02

CHINESE DATA PRIVACY LAW UPDATE AND BEST COMPLIANCE PRACTICE FOR MULTINATIONAL CORPORATIONS

Why Personal Information Protection Matters in China

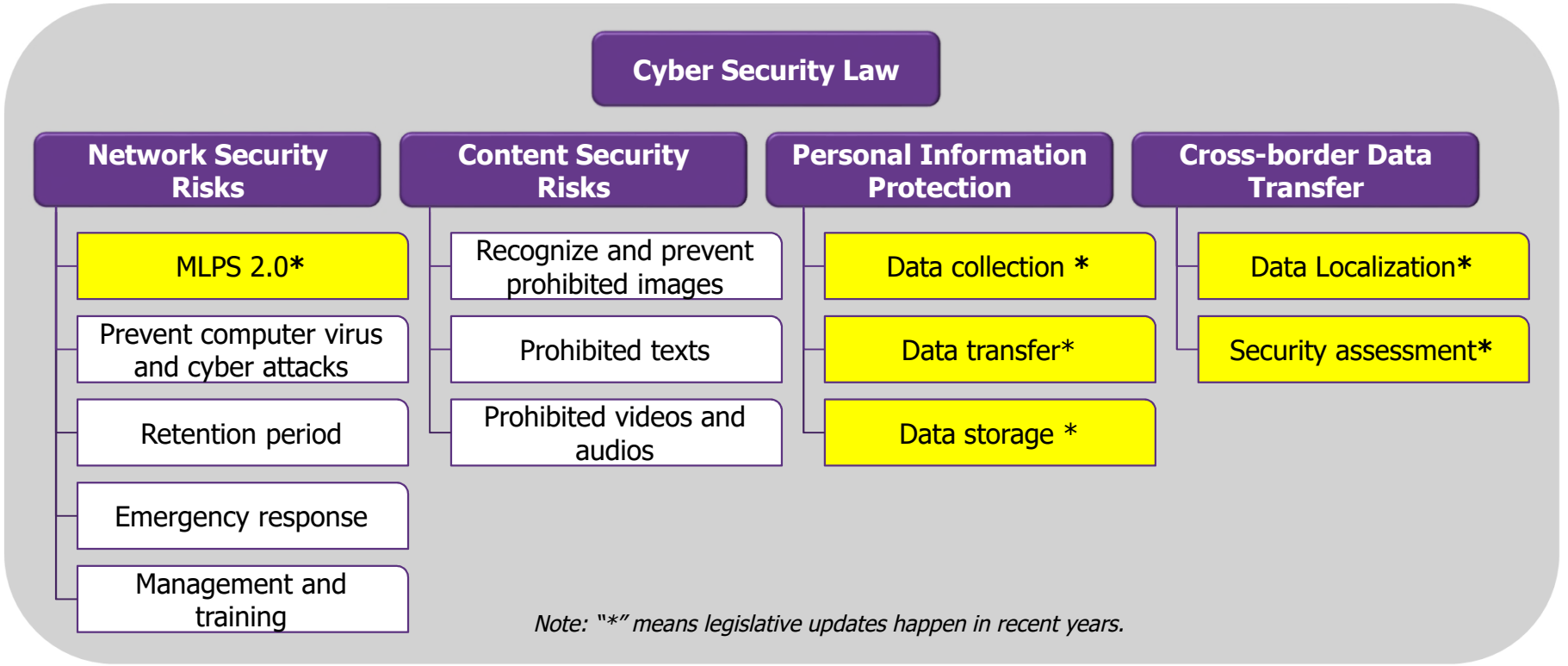
Wide application scope

- Cyber Security Law imposes information protection obligations on all network operators.
- It applies to all organizations in China that provide services over the internet or other information network, including internal networks and systems, such as the company's HR systems.

Broad definition of personal information

- Information that could "identify" a person
  - Such as a person's name, address, telephone number, date of birth, identity card number and biometric identifiers
- Information that could be "linked" to a person
  - Once an individual is identified, any other data generated by this person in his or her following activities also constitutes personal information
  - Such as a person's location, communications records, and individual's online browsing history

Chinese Data Protection Framework



General Requirements under Chinese Data Protection Laws

Data collection & processing

- Principles: Lawful, Justifiable and Necessary
- Notification and consent requirements
  - Employee notice/client notice/online privacy policy

Security of data

- Keep collected personal data safe and in strict confidence
- Multi-Level Protection Scheme (MLPS 2.0): the requirements to follow the MLPS 2.0 series standards and conduct MLPS compliance implementation

Transfer of data

- Notification and consent requirements
- Data localization and security assessment requirements for cross-border data transfer

Legislative Updates - Personal Information Protection

Key updates

- Specifications - bridging the gap between data privacy principles laid out in CSL and practice.
- Administrative Measures on Data Security - will be the first binding administrative regulation on personal information and important data protection following the effectiveness of CSL.
- Notable Changes:
  - A forced "unbundling" of consents: requiring separate and explicit "opt-in" consent to each purpose for which personal data is being processed
  - Area of particular concern: advertisement personalization and other form of digital marketing - potential impact on online business model that derive commercial benefit from data analytics and data sharing.

Data localization and cross-border data transfer

- Under Article 37 of CSL, CIIOs are required to store personal data and important data within PRC territory. In case of a cross-border data transfer, CIIOs are subject to a security assessment conducted by the Cyberspace Administration of China (CAC). Cross-border data transfers that may bring risks to the national security, public interests or data subjects' rights are not allowed.

CIIO	Entities in critical information infrastructure industries whose damage, loss of function or data leakage of their network system would seriously harm China's national security, national economy, people's livelihood, and public interests
Personal Information	Information that could "identify" a person or be "linked" to a person
Important Data	Data that if disclosed, would impact national security, economic security, social stability, public health and safety, such as non-public government information, significant volumes of data related to finance, population, genetics and health care, geographic, and mineral resources

Data localization and cross-border data transfer

Examples of CIIs:

- The CSL provides examples of CII, including network operators in the areas of public communications, information services, energy, transportation, water utilities, finance, public services, and e-government, but leaves the specific definition of CII to the regulations to be made by the State Council.
- The Regulation for the Security Protection of the Critical Information Infrastructure (Consultation Draft) defines the scope of CII by listing operators in certain industries, including
  - government agencies and entities in the energy, finance, transportation, water conservation, healthcare, education, social insurance, environmental protection, and public utilities sector;
  - information networks, such as telecommunication networks, broadcast television networks, and the Internet, and entities providing cloud computing, big data, and other large-scale public information network services;
  - research and manufacturing entities in sectors such as science and technology for national defense, large equipment manufacturing, chemical industry, and food and drug sectors; and
  - press units such as broadcasting stations, television stations, and news agencies.

Data localization and cross-border data transfer

Examples of important data in 27 industries and sectors:

- oil and natural gas, coal, petrochemical industry,
- electric power, telecommunications, electronic information,
- iron and steel industry, nonferrous metals,
- equipment manufacture, chemical industry,
- national defense, other industries that have national security implications,
- geographic information,
- civil nuclear facilities, transportation, post express, water conservancy,
- population health, finance, credit, food and medicine, statistics, meteorology,
- environmental protection, broadcasting, marine environment,
- e-commerce,
- a catchall category for any other data in any other area that may affect the peace, prosperity, or social welfare of China.

The definitions, scope, and identifying criteria of important data in these key industries may be further specified by the competent industry regulators or regulatory authorities.

Data localization and cross-border data transfer

- A legislative trend - draft regulations, such as the Measures for Security Assessment for Cross-border Transfer of Personal Information, extend data localization requirements to all network operators.
- If draft regulations come into force, all network operators should conduct a security assessment before transferring personal data and important data outside China.
  - "Network operator" is more broadly defined than CIIO.
  - MNCs' use of networks in China to transfer data within an internal cross-border network may also constitute a cross-border transfer, such as data transfers between the domestic subsidiary and oversea headquarter.
  - Foreign entities that are not registered in China may also be required to perform a security assessment for cross-border data transfer if they provide products or services within China.
    - Consideration factors include: whether Chinese language is used, whether the payment is made in CNY, and whether the products or services are delivered to China.
    - Foreign entities should fulfill the obligations through their legal representatives or institutions in China.

Legislative Updates - Multi-Level Protection Scheme

- Network operators are required to classify their network and information systems into different levels based on the level of importance of their network systems to national security, economic and social life, with 1 being the least sensitive, 5 being the most.
- The higher the ranking, the more monitoring by MPS as well as third-party certification, MPS filing, and annual reviews.
  - Level 3, the point at which self-certification turns into government reviews, happens when damage to the networks would, among others, "cause extremely serious harm to rights and interests of individuals, legal persons and other organizations, cause serious harm to social order and the public interest, or cause harm to national security."
  - Networks rated level 3 and above are required to put in place enhanced policies and procedures, such as cybersecurity monitoring, detection and response, and incident notification to relevant authorities.
    - Level 3 network operators are required to conduct national security reviews for the procurement of network products and services if they may affect national security.
    - They will be inspected by government officials at least once a year.
    - Their networks must also be technically maintained in China rather than remotely maintained from overseas. If work must be done from overseas, it must undergo a cybersecurity review and be logged in case of inspection.

Legislative Updates - Multi-Level Protection Scheme

Key updates: 1.0 vs 2.0

- **Application scope broadened** to include Basic Information Network, Cloud Computing Platforms/Systems, Big Data Applications/Platforms/Resources, Internet of Things ("IoT"), Industry Control Systems, Mobile Interconnection Systems
- **Level 3 criteria expanded** to include rights and interests of individuals, legal persons and other organizations
- **Cyber grading requirements enhanced** in terms of:
  - Expert review
  - Technical maintenance requirement

Penalties & Enforcement

Act. 59	Act. 60	Act. 61	Act. 64	Act. 68
Failure to perform network security protection duties	Failure to immediately take remedial measures for security flaws and vulnerabilities	Failure to require users to provide truthful identity information	Infringe on personal information	Failure to stop transmission of prohibited information
Fine: Between RMB 10,000 to 100,000	**Fine**: Between RMB 50,000 to 500,000	**Fine**: Between RMB 50,000 to 500,000. A temporary suspension of operations, closing of website, and cancellation of business licenses	**Fine**: Between 1 and 10 times the amount of unlawful gains. A temporary suspension of operations, closing of website, and cancellation of business licenses	**Fine**: Between RMB 100,000 to 500,000. A temporary suspension of operations, closing of website, and cancellation of business licenses

The most severe penalties for network operators is usually suspension of business or shut down of website.

Practical Implementation

Audit personal information collected

- How will the data be collected?
- Why is it being collected?
- Where will it be transmitted to?
  - To an affiliate who will continue to independently analyze the data?
  - To a data processor who has no discretion to conduct further analysis?
- What are the rights of the data subjects?
  - Does processing cease if the data subject requests?
  - Do data subjects have access and correction rights?
- Storage and maintenance
  - Where will the data be stored?
  - Is the security adequate?
  - How long will the data be kept?
  - How will it be destroyed when no longer needed?

Practical Implementation

Comply with laws and regulations

- Local regulations
- China: security assessment of personal information and important data
- Regulations where the data is being transferred

Continuing compliance issues

- Personal information collection statements and informed consent forms
- Data processing policies and procedures
- Data anonymization procedures when required
- Outsourcing compliance issues
- Data breach management and notification
- Crisis response

Continuous improvement and adaptation to changes in law

Key Takeaways

- Assess the scope of data during early case assessment, including, incorporating steps to identify and categorize the data during data collection.
- Whenever possible, collect, filter and review data in the PRC, or at the very least, filter and screen the personal information and important data in China before transferring them.
- Execute and implement data transfer agreements between entities/offices.
- Redact or anonymize personal information wherever feasible.
- Conduct self-assessment of risks and security measures, and document any steps taken to protect the data subjects' privacy and comply with the applicable data privacy laws.
- Report security incident to CAC or Public Security Bureau timely.

SECTION 03

RECENT ENFORCEMENT PRACTICE OF THE RUSSIAN DATA PROTECTION AUTHORITY (ROSKOMNADZOR)

General Background

- Federal Law No. 152-FZ "On Personal Data" (the "**PD Law**") of 2006:
  - **personal data** is any information directly or indirectly related to an identified or identifiable individual
  - no concepts of "data controller" and "data processor"
  - "**data operator**" is a person that organizes or carries out (alone or together with other persons) the processing of personal data and determines the purposes of processing
  - data processing can be delegated to a **third party**, who will be acting under the authorization or "**instruction**" of the data operator
- Certain provisions of the PD Law apply to the data operators and third parties that have no legal presence in Russia but target Russian customers
- The Federal Service for Supervision of Communications, Information Technology and Mass Media, or **Roskomnadzor**, is the data protection authority

Russian Law Requirements

- Valid grounds for data processing
  - individual's consent is required in most cases
  - concept of "legitimate interest" of data operator is still developing
- Organizational measures
  - detailed internal policies and procedures including regular audit
  - appointment of DPO is obligatory
- IT measures
  - scope of security measures (both hardware and software) is specifically regulated by law
  - "localization requirement"
- Notification to Roskomnadzor on data processing activities

Localization Requirement

- Starting September 2015 Russian citizens' personal data must be recorded, stored, amended and extracted using databases **physically** located in Russia
  - cross-border transfers are allowed
  - cloud solutions?
- Starting November 2017 LinkedIn is being blocked for access for Russian IP-addresses
- Starting December 2019 penalties for violation of localization requirement are dramatically increased up to $83,000 for initial violation and up to $249,000 for repeated violation
- In February 2020 two major social media companies were fined for failure to comply with localization requirement for $63,000 each

COVID-related Data Processing

- Roskomnadzor issued several official interpretations
  - processing of sensitive data about individuals' health conditions is allowed without individuals' consents
  - processing of health information for the purposes of state authorities is allowed including publication of sensitive data
- A new law establishing a special legal framework for the development and adoption of AI technologies in Moscow for the period from 1 July 2020 to 1 July 2025
  - legal entities and entrepreneurs can be included in a special public register maintained by Moscow authorities
  - Moscow authorities have been authorized to introduce detailed regulations on the development, adoption and sale of AI technologies and AI-based products and services
  - additional rules on the processing of anonymized personal data

SECTION 04

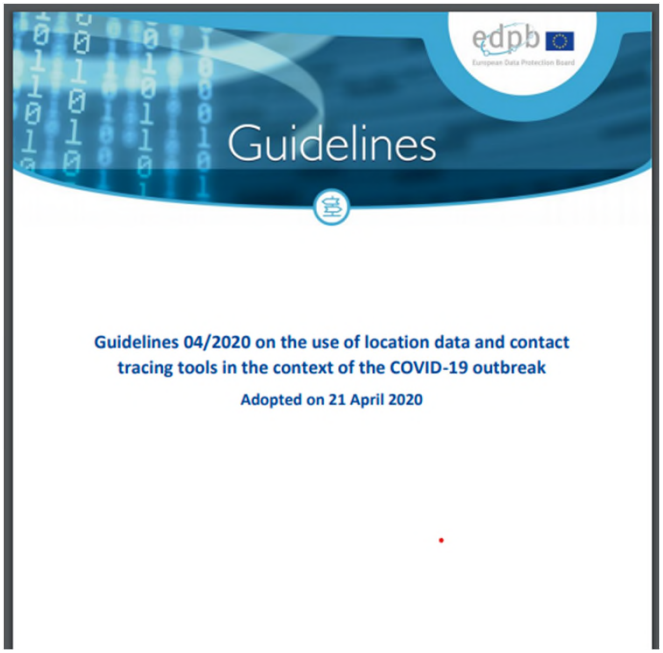
INTERNATIONAL DATA TRANSFERS AFTER COVID-19 AND NEW EU STRATEGY FOR DATA

Personal data transfers from the EU after COVID 19

- The **available legal tools for data transfers** will continue to exist, unless the ECJ steps in with a ruling.
  - EU Standard Contractual Clauses (for data processors or controllers in the U.S., not for controllers in the U.S. and processors in the EU)
  - EU-US Privacy Shield/Swiss-US Privacy Shield (currently 4,000 + US companies registered)
  - Unambiguous consent of the data subject (high hurdle).

  → **international COVID 19 data base?**

  - *"The EDPB generally considers that data and technology used to help fight COVID-19 should be used to empower, rather than to control, stigmatise, or repress individuals."*



Consent: Not Easy to Get

- Must be revocable at any time
- Must be fully documented
- Must be given freely
- No "implied" consent allowed
- Frequently becomes an issue in the health care area
- EC discourages the use of informed patient consents as the sole legal base for collections of health data (Art. 9 GDPR) and data transfers into the U.S. → EDPS Opinion 1/6/20

EU/US Standard Contractual Clauses ("SCC" or Model Clauses)

- Full Fledged contracts – not just "clauses"
- Cumbersome – most recent version from 2010
- Third party beneficiary rights, venue in the EU
- **Review of European Court of Justice pending** - Schrems II case
- Judgment scheduled for **July 16.**
- 12/19/19: Advocate General Henrik Saugmandsgaard Øe ("AG") suggests that
  - there is "nothing to affect the validity of EU Decision 2010/87" – the European Commission's decision of February 2010 on the SCC
  - "the validity of that decision does not depend on the level of protection that exists in each third country to which data might be transferred" (e.g. on U.S. law).
- If the ECJ rules against the AG → thousands of data transfer agreements that use the SCC and that have relied on the EC decision for almost 10 years affected.

EU/US Privacy Shield

- Proceeding pending at the European Court of Justice (Schrems II - C-311-18)

  The AG has "doubts about the validity of the finding that the United States guarantees, in the context of the activities of their intelligence services on the basis of section 702 of the FISA and EO 12333."

- Recertification required, annual fees for small businesses
  - $375 for certification
  - $250 for Privacy Arbitral Fund
  - $750 or more-annual enrollment fee for dispute resolution
- U.K. needs to be added as a separate country because of BREXIT.

EU/US Privacy Shield (II)

- ECJ will follow the AG or be **more proactive**, especially with regard to the EU's Privacy Shield decision of 2016 that it could declare entirely or partially invalid.
- If one DPA alone would **suspend data flows to the U.S. under the SCC** that would create havoc within the EU industry. Such a drastic measure is only imaginable that a DPA in specific cases:

➢ The EU decision underlying the SCC will probably survive the scrutiny of the ECJ, BUT **DPA will still play in important role in the GDPR compliance process and SCC "on a case-by-case basis."**

➢ **Open: Fate of EC's Privacy Shield decision of 2016,** although the EC has endorsed it on several occasions and is working with the US Government to address deficiencies.

EU Data Strategy – Released: Feb. 19, 2020

- **Where?** EC "Communication" – 35 pages
- **Vision?** "Making the EU a role model for a society empowered by data."
- **Time line?** Strategy until 2030, but EC needs support of the Member States

How to achieve this goal?

- "[By] setting clear and fair rules on access and reuse of data
- Investing in next generation standards, tools and infrastructures to store and process data
- Joining forces in European cloud capacity
- Pooling European data in key sectors, with EU-wide common and interoperable data spaces
- Giving users rights, tools and skills to stay in full control of their data."

2021-2027 → EC will invest in a **"High Impact Project"** on European data spaces and cloud infrastructure (Planned EU €2 billion investment share).

EU Data Strategy (I) Opportunities for US Companies

- Participate in investments/subsidies for next-generation technologies and infrastructures (EU Open Data Portal, Horizon Europe and Digital Europe programmes for SME)
    - Focus: computing/quantum computing, cyber-security, low-power processors, 6G networks, European Open Science Cloud (EOSC), Green Deal data space, mobility data space, energy data space
- European data pools enabling Big Data analytics and machine learning
- More Government-to-business – G2B – data sharing

EU Data Strategy (I) Opportunities for US Companies (Continued)

- Example Personalized medicine and Blockchain technologies
- High level of cybersecurity through EU Cybersecurity Certification
- Framework and the EU Agency for Cybersecurity (ENISA)
- Make use of data portability rights (Art. 20 GDPR) to attract customers
- Opportunities to set industry standards (e.g. Cloud computing)

EU Data Strategy (III) Challenges

- Fragmentation within the EU will remain, e.g. for G2B data flows
- Data interoperability and diverging data quality
- Data Storage in the EU, not required by desired
- Example of Challenges: EU-based cloud providers have only a small share of the Cloud market → “high dependency on external providers” + “vulnerability to external data threats” + “loss of investment potential for the European digital industry in the data processing market”
- Restrictions for non-EU equipment manufacturers (e.g. 5G)

EU Data Strategy (III) Challenges

- Impact of GDPR, Cybersecurity Act and a future Data Act unclear (Cloud Rulebook delivered by Q2 2022?)

- EU-US/China Trade disputes: EC committed to promoting and protecting European data processing rules and standards→ sharing of data only with trusted countries + “promote the European model around the world”


SECTION 05
TAKEAWAYS

Key Takeaways

1. Stringent global privacy laws are continuing to evolve.

2. Key differences e.g. localization laws, government access to data, data transfer and restriction considerations.

3. COVID-19 challenges for:

   a. health data collection and data use when managing infections of staff and planning the return to work;

   b. contact tracing apps and similar technologies; and

   c. Managing data processing issues and breaches in the lockdown

4. The legal landscape does keep evolving!

Pulina Whitaker

Pulina Whitaker
London
+44.20.3201.5550
pulina.whitaker@morganlewis.com

Pulina Whitaker is a co-leader of the Firm's Privacy & Cybersecurity practice. She specalizes in both labor and employment matters as well as data privacy and cybersecurity. She manages employment and data privacy issues in sales and acquisitions, commercial outsourcings, and restructurings. Her global data privacy practice includes handling data breach incidents, managing cross-border transfers of personal data, and advising on privacy and website cookie notice and consent requirements, internal and external privacy policies, data processing consent requirements, and the implementation of data subject rights. She has extensive experience working with international and European clients to comply with the Euroepan General Data Protection Regulation, including advising on audits of data processing activities and data security incidents.

Todd Liao

Todd Liao
Shanghai
+86.21.8022.8799
todd.liao@morganlewis.com

Todd Liao works with clients on a wide range of financial transactions and legal issues involving China. He frequently works with multinational corporations on cross-border mergers and acquisitions, foreign direct investment and investment financing, disposal of Sino-foreign joint ventures and assets, and the structuring of complex commercial transactions. He advises multinational corporations regarding compliance with the FCPA and other regulatory compliance matters including policies and practices, gifts, travel and entertainment policies and violations, third-party due diligence issues, managing and conducting investigations of alleged FCPA violations, whistleblower investigations, and employee disciplinary actions. He also conducts FCPA training in multiple languages.

Ksenia Andreeva

Ksenia Andreeva
Moscow
+7.495.212.2527
ksenia.andreeva@morganlewis.com

Ksenia Andreeva specalizes in both intellectual property and cybersecurity matters. Ksenia's practice is focused on complex data protection and compliance matters, including international data transfers and security projects. Ksenia assists clients with every aspect of compliance implementation, including conducting risk assessments, evaluating and enhancing existing data protection compliance programs, making improvements to internal controls and processes, and conducting employee trainings. Ksenia is a member of the Advisory Board of the Russian Data Protection Authority (Roskomnadzor).

Dr. Axel Spies

Dr. Axel Spies
Washington, DC
+1.202.739.6145
axel.spies@morganlewis.com

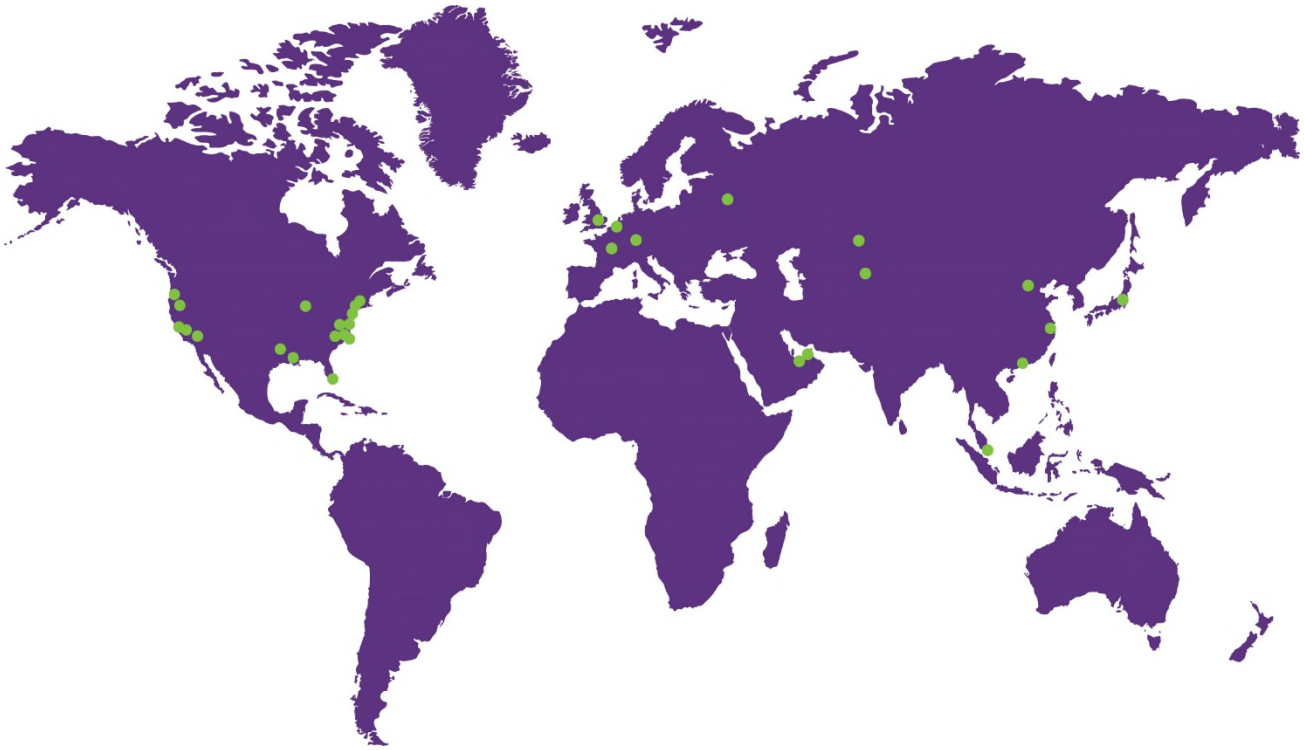
Dr. Axel Spies has advised clients for many years on various international issues, including licensing, competition, corporate issues, and new technologies such as cloud computing. He counsels on international data protection (EU General Data Protection Regulation), international data transfers (Privacy Shield), healthcare, technology licensing, e-discovery, and equity purchases. A member of the Sedona Conference on Electronic Discovery, Dr. Spies is frequently quoted in the media for his telecommunications and privacy knowledge

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU