Morgan Lewis

DATA TRANSFERS IN THE EU, RUSSIA AND CHINA

Pulina Whitaker, Dora Wang and Ksenia Andreeva

May 14, 2018

SECTION 01

DATA TRANSFER IN EU

The New EU General Data Protection Regulation

- New GDPR will replace existing EU Data Protection Directive for commercial data privacy obligations starting 25 May 2018
- Expanded application of the EU data privacy obligations
- The GDPR will apply to processors and controllers having an EU-based establishment where personal data are processed in the context of the activities of this establishment
- The GDPR will also apply to controllers and processors based outside the EU territory where the processing of personal data regarding EU data subjects relates to:

    - the offering of goods or services (regardless of payment)

    - the monitoring of data subjects' behavior within the EU

- "Personal Data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person
- Personal data still to be processed fairly and lawfully

The New EU General Data Protection Regulation, cont'd

- Data Protection Officer: for controllers/processors processing substantial sensitive personal data or who have core activity of monitoring individuals on a large scale or public body
- Right to request to be forgotten, have data rectified or deleted
- Privacy by design: privacy safeguarding technology built-in from the start
- Actively factor privacy considerations into the design and upgrade of all systems, policies, settings which process personal data
- Privacy by default: privacy-friendly default settings until user chooses otherwise
- Data protection impact assessment: prior to processing if high risk for individuals
- Notify data breach to DPA without undue delay/within 72 hours and to individuals without undue delay if there is likely to be high risk to individuals
- Penalties for breach of GDPR – up to higher of 4% global turnover or €20,000,000
- Controllers and processors will be directly liable under GDPR
- Local laws in each EU / UK country

Data Transfers under GDPR

- General restriction on transferring personal data outside EEA to a "third country"
- Adequate countries: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay (Japan and South Korea under consideration)
- GDPR permitted data transfer options (safeguards):
  - Binding Corporate Rules
  - Standard contractual clauses: importer controller/processors based in the third country; exporter controller must be based in Europe
  - Importer subject to an approved Code of Conduct
  - Importer subject to an approved certification mechanism (e.g. Privacy Shield)
- GDPR permitted derogations:
  - Explicit consent
  - transfer is "necessary" for performance of contract; to establish, exercise or defend legal claims; from a public register
  - Where the transfer is not repetitive, concerns a limited number of data subjects, is necessary for compelling legitimate interests of controller (not overridden by data subject rights) and safeguards in place to protect the data

Which data transfer option?

- Privacy Shield – green light last year for EU/Switzerland to US transfers
- Standard contractual clauses – easy to execute; not so easy to implement?
- BCRs – time and expense to get approval
- Consent – GDPR standard of explicit consent
- Other new options: Code of Conduct, privacy seals – details awaited from supervisory authorities
- Give notice to data subjects of the transfers

SECTION 02

DATA TRANSFER IN CHINA

PRC Data Privacy Law Framework

Before 2017: No Unified Legislation (approximately 40 laws, 30 regulations, 200 industry-specific rules)	
General Law	The Decision of the Standing Committee of the National People's Congress on Strengthening the Network Data Protection (NPC Decision)
	Provisions on Protecting the Personal Data of Telecommunications and Internet Users
Specific Law	Consumer Rights Protection Law of the People's Republic of China
	Medical Records Administration Measures of Medical Institutions
	Measures for Administration of Population Health Data (PHI Measure)
	Implementing Regulations of the Drug Administration Law of the People's Republic of China
Penalty Provision	Notice of the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security on Penalties for Criminal Activities Related to Infringement of Personal Data of Citizens
	Ninth Amendment of the PRC Criminal Law
	Measures for Penalizing Infringement on Consumer Rights and Interests (issued by the SAIC)

PRC Data Privacy Law Framework

After 2017: PRC Cybersecurity Law ("CSL"): First unified legal regime on data privacy	
Responsible Authority	Cyberspace Administration of China ("CAC")
Effective Date	China Cybersecurity Law ("CSL") took effect on June 1, 2017
Draft Implementation Measure for Comments	Measures on Security Assessment of Cross-border Data Transfer of Personal Data and Important Data
Draft Guideline for Comments	Data Security Technology - Guidelines for Data Cross-Border Transfer Security Assessment (Guideline)
Draft Guidance for Comments	Information security technology - Guidance on De-Identifying Personal Information (8/15/2017)
National Standard on Personal Data Protection	Information Security Technology – Personal Information Security Specification ("PISS") (Effective May 1, 2018)

Penalties under CSL

Administrative Order

- Violators may be warned and ordered to make rectifications by the competent authority;
- Serious violations could lead to suspension or revocation of business licenses

Fine

If a violator refuses to make rectifications or in the event that the cybersecurity breach causes severe damages to the network, the network operator and/or its individual-in-charge will be fined.

The operator: ranging from 10,000 yuan to 100,000 yuan

The supervisor: directly in charge: ranging from 5,000 to 50,000 yuan

Other

In the even that an emergency or a security accident occurred due to cybersecurity breaches, the following laws and regulations may apply:

- The Emergency Response Law of the People's Republic of China
- The Law of the People's Republic of China on Work Security
- Other related laws and regulations

Key Provisions of CSL and its Supplemental Guidelines

1. Who is subject to CSL?

Network Operator

Network Operators: Owners or administrators of networks or network service providers

Catch-All: Business entities that provide services and conduct business operations using networks

"CIIO"

CIIO: refers to operators in certain industries related to public communication, data services, energy, finance, transportation, water conservation, public utilities, digital governance or any other business, that, if it is destroyed, its functionality compromised, or its data leaked, could compromise national security and welfare, national economy, and public interests

① CAC retains broad discretion to interpret the last "catch-all" category

① CIIOs are subject to heightened security requirements

Key Provisions of CSL and its Supplemental Guidelines (cont'd)

2. What constitutes protectable data under CSL?

Personal Data

Information that can identify the data owner, such as name, birth date, ID number, address, telephone number, bank account number, transaction information, location data, etc.

Sensitive Personal Data

Personal data that, if it is leaked or illegal provided to other parties or misused, will endanger the personal safety or property security or harm personal reputation or physical or mental health, or will lead to discriminatory treatments. E.g., ID, property information, health record, biometrics, location data are considered sensitive personal data, personal information of children under age of 14

Important Data

Data closely related to the national security, economy developments and social interests

Handling Data under CSL

Consider

- types of data
- sensitivity and importance of the type of data collected
- quantity of data
- risk of data misappropriation
- security breach
- ramifications of a data breach

Prioritize

- Review and strengthen network security systems and protocols that need to be implemented
- Review IT infrastructure and data mapping

Take Action

- Review clauses in commercial contracts related to data collection and transfer
- Assess data-related protocols employed by subsidiaries and business partners to ensure that the content and approach of the data collection, storage, use and transfer comply with the new law
- Review company policies and employee handbook for employee consent under the law

Handling Data under CSL (cont'd)

Collection & Use → **Data Storage** → **Cross-Border Data Transfer**

- Obtain true identities of users; inform data subjects of privacy policy; obtain consent in advance; principle of necessity: scope to be limited to only what is necessary for legitimate purpose;
- Issue notification to users and to the competent authorities of any data losses or security beach

- CIIO – personal information and other important data should be stored domestically on servers that are physically located in China (a possible grace period until the end of December 2018).

- Express consent
- Two-tiered security assessment

Cross-Border Data Transfer under CSL

Express Consent

How to obtain consent?

- Provide a full disclosure of the purpose, scope, content, receiving entity and the countries or regions where the receiving entities are located
- Obtain explicit consent in writing (highly recommended)
- Consent is given by data subjects' making international phone calls, sending emails or instant messages to individuals or organizations overseas

Two-tiered Security Assessment

What should network operators do?

- annual security self-assessment
- reassessment if there is any material change

What should CIIO do?

- submit to additional regulatory assessment conducted by competent authorities

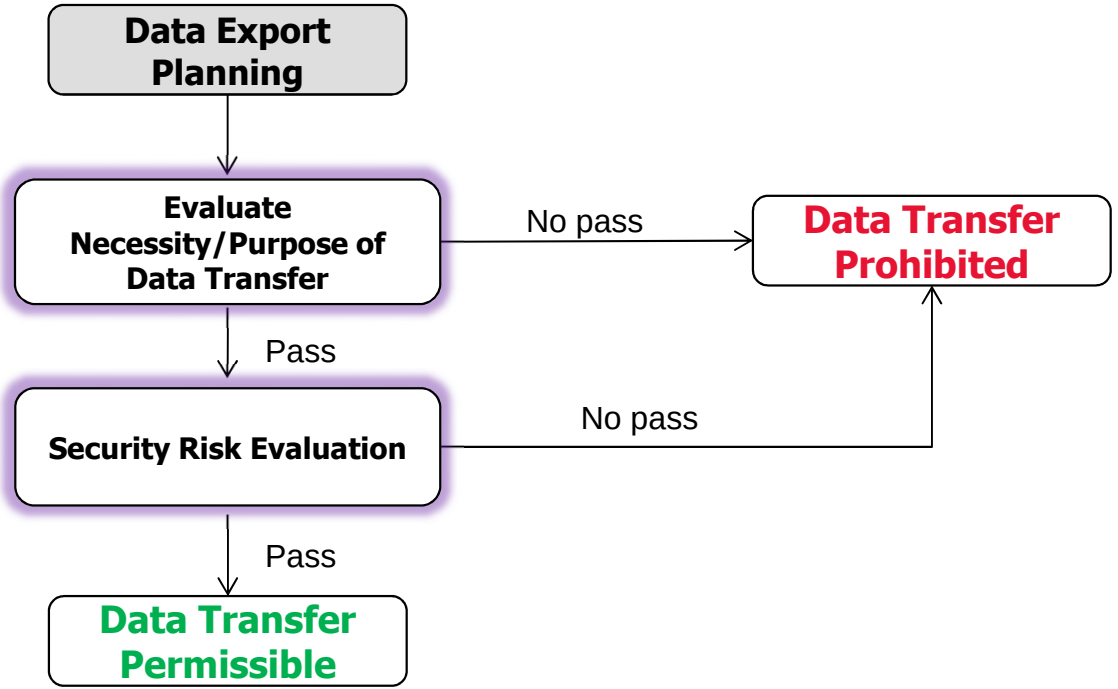
Other Permissible Ways to Transfer Data Overseas

- anonymize or de-personalize data; transfer with legitimate business necessity

Prohibited Cross-Border Data Transfer

- The owner of personal information has not given explicit consent to the cross-border transfer or the transfer may jeopardize personal interests;
- The outbound transmission posts security risks to national politics, economy, technology and defense, which may affect national security and jeopardize social and public interests; or
- Other data which are prohibited to be transferred abroad as determined by the CAC, MPS, security authority and other relevant authorities.

Cross-Border Data Transfer – General Assessment



Data Transfer Subject to Regulatory Assessment

- More than 500,000 people
- Exceeds 1000 GB
- Involving nuclear facilities, chemical biology, defense and military industry and population health, data on large engineering projects, marine environment and sensitive geographical information, etc.
- Involving vulnerabilities and security protection of CII
- Operators of CII
- Other data possibly affecting national security and social public interests

Cross-Border Data Transfer – Regulatory Assessment

- necessity and purpose of the cross-border transfer of the data
- importance or sensitivity of data to be exported
- risk of data being leaked, destroyed, modified, or misused
- risk to national security, social welfare and public interests due to data export
- security measures implemented by the data recipient
- adequacy of the emergency response plan
- level of expertise / sufficient training of security personnel
- response / investigation of threats of data breach/complaint of breach
- security breach notification mechanisms

SECTION 03

DATA TRANSFER IN RUSSIA

Data privacy regulations in Russia

- Federal Law No. 152-FZ "On Personal Data" of 2006
  - based on the EU Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
  - personal data is any information directly or indirectly related to an identified or identifiable individual
  - no concepts of "data controller" and "data processor"
  - concept of "data operator", 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 Personal Data Law may apply to the data operators that have no legal presence in Russia but target Russian customers
  - localization of data processing activities
  - requirements on the transfers of the Russian citizens' personal data

Localization requirement

- Mandatory requirement to use "Russia-based databases" to record, systematize, accumulate, store, update and modify, and retrieve Russian citizens' personal data
  - either use a database on a server, which is physically located in Russia (the use of the cloud-based services is a gray area)
  - engage a local partner to collect personal data on behalf
- The requirements on personal data localization do not impose any additional restrictions on cross-border transfer of personal data located in Russia
- Failure to comply with the localization requirement may lead to the blocking of Internet website or application for access of Russia-based IP addresses

Requirements on data transfers

- Major requirements:
  - localized "primary" database
  - consent of data subject on the transfer
  - data transfer agreement
- Consent of data subject on the transfer
  - all countries that are signatories to the Strasbourg Convention are considered to be jurisdictions that provide "adequate protection" of the rights and interests of data subjects
  - the Russian Data Protection Authority (Roskomnadzor) issues a list of countries that provide "adequate protection"
  - transfers to the countries that do not provide adequate protection require **written** consent of individual, unless one of the exemptions applies

Consent on cross-border data transfers

- No prescribed form of consent, but the law provides for following information to be included in the consent form:
  - Full name and ID number of the individual
  - Data operator details (i.e., full company name, address and state registration numbers)
  - Company details of **all** companies which may have access to the transferred data (either the data operator's group or third parties)
  - Purpose of the data transfer
  - List of personal data to be transferred
  - Duration of individual's consent, and the method of its withdrawal (i.e., contact details of the data operator's data protection officer)
- Consent may be provided as a part of the agreement (e.g., terms and conditions, services agreement)

Consent on cross-border data transfers, cont'd

- Consent of individual on cross-border data transfer is not required, if
  - data transfer is allowed under an **international treaty** that Russia is a party to
  - data transfer is allowed under applicable laws if necessary for the purposes of protecting the Russian constitutional system; or protecting the national **state defense and state security**, or securing the maintenance of the Russian transportation system, and protecting the interests of individuals, society and the state in the transportation sector from illegal intrusion
  - data transfer is **only** made for perform an agreement to which an individual is a party to
  - data transfer is required to protect the individual's life, health or other vital interests and it is impossible to obtain his prior consent in writing
- **Where possible, obtain explicit consent of individual on the transfer of his/her personal data**

Data transfer agreement

- Data transfer agreements (= "data operator's instructions")
- Roskomnadzor has not adopted a standard form of a data transfer agreement
- Roskomnadzor's advice on the best practices on the data transfer agreement
  - clear and detailed rules on data processing to be conducted by a third party
  - purposes of processing and possibility of further transfer
  - scope of organizational measures to be taken by a third party processor
  - scope of security measures to be taken by a third party processor (e.g., use of certified software or encryption)
  - regular audits by the data operator
  - contractual liability limitations

SECTION 04

CASE STUDY

Case Study – Multijurisdictional Considerations

- MegaMine is a U.K. multinational company with subsidiaries in various countries, including China and Russia. MegaMine conducts geological surveys of mines and sells the data to research institutes, government or other business entities all over the world. MegaMine generally stores its survey and customer information on servers located in the UK, while most of its HR-related data is stored in a server in China.
- John is a sales executive who has worked for MegaMine in London since 2016. In 2017, John spent 5 months in Russia working on a survey project, helping investors from China assess the value of a particular gold mine that was targeted for sale. The transaction went through. The Chinese investors were pleased with the result; and John was promoted.
- In January 2018, John took a transfer opportunity to be the general manager of MegaMine's subsidiary in Beijing. However, shortly after he took the position, a whistleblower reported to the company's ethics hotline that John helped the Chinese investors pay bribes to obtain the license to operate the gold mine and that he frequently entertains the Chinese investors at luxury resorts in China.
- MegaMine's legal teams in London and APAC legal counsel in Hong Kong want to collect and analyze all transactions and travel and entertainment records related to the Chinese investors and John's reimbursement and sales records. John has kept one company laptop for all of his personal and business use since 2016, and he only infrequently saves documents or emails onto the company's servers. MegaMine's legal team needs to quickly image, collect, and analyze data on John's laptop in addition to data on the servers in London and China for investigation purposes.

Case Study – Multijurisdictional Considerations

- Assuming MegaMine does not already have a sufficiently robust consent clause or data privacy disclosure in HR and transaction documents for its employees and/or customers for the cross-border data transfer, what are the risks associated with this transfer?
- How can MegaMine's legal team mitigate the risks with respect to the investigation now?
- What can MegaMine do to mitigate its regulatory risks in UK, China, and Russia with respect to cybersecurity and data privacy law of each jurisdiction going forward?

Morgan Lewis Technology May-rathon 2018

Morgan Lewis is proud to present Technology May-rathon, a series of tailored webinars and in-person programs focused on current technology-related issues, trends, and legal developments.

This year is our 8th Annual May-rathon and we are offering over 25 in-person and virtual events on topics of importance to our clients including issues of privacy and cybersecurity, new developments in immigration, employment and tax law, fintech, telecom, disruptive technologies, issues in global tech and more.

A full listing and of our tech May-rathon programs can be found at https://www.morganlewis.com/topics/technology-may-rathon

Q&A

Thank you for running in the 2018 Technology May-rathon with us.

We would be pleased to answer your questions.

The Q&A tab is located on the bottom right hand side of your screen. Please type your questions in the space provided and click Send.

Biography

Dora Wang
Partner
Shanghai/Beijing, China
T +86.21.8022.8576
dora.wang@morganlewis.com

Dora Wang advises multinational corporations in a broad range of industries on regulatory and compliance matters, complex cross-border litigation and commercial dispute resolution, government and internal investigations, and employment disputes.

Dora regularly counsels companies on advisory and investigation matters involving cybersecurity and data privacy law, anti-corruption laws (US Foreign Corrupt Practices Act, UK Bribery Act, and local anti-corruption requirements), antitrust/competition laws, third-party due diligence, compliance audit and risk assessment, policy formulation and implementation, and contentious employment matters such as labor arbitration, employee disciplinary actions, and collective bargaining negotiations.

Biography

Pulina Whitaker
Partner
London, UK
T +44.20. 3201.5550
pulina.whitaker@morganlewis.com

Pulina Whitaker's practice encompasses 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. Pulina provides day-to-day advisory support for multinationals on all employment issues, including the UK's Modern Slavery Act and gender pay reporting requirements. She also advises on the full spectrum of data privacy issues, including preparing for the General Data Protection Regulation. Pulina has deep experience managing international employee misconduct investigations and has been appointed as a Compliance Monitor for a transnational organization.

Biography

Ksenia Andreeva
Partner
Moscow, Russia
T +7.495.212.2527
ksenia.andreeva@morganlewis.com

Ksenia Andreeva specializes in intellectual property (IP) matters. She advises on a wide range of transactional, regulatory, and commercial IP matters as well as disputes and enforcement of IP rights.

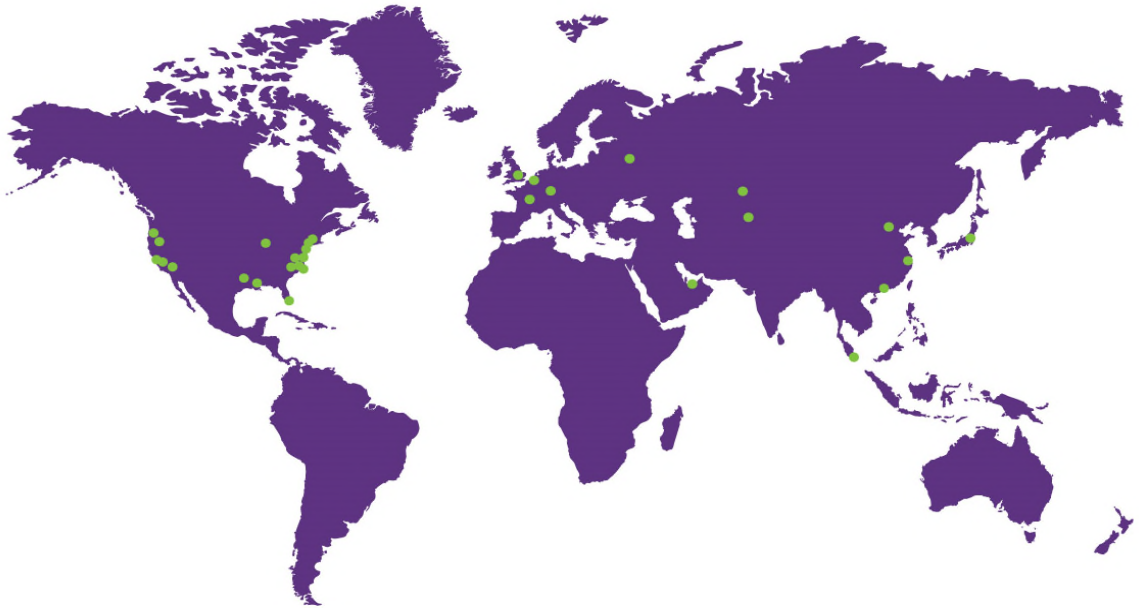
Ksenia is a registered trademark attorney and is admitted to represent clients before the Russian Patent and Trademark Office (Rospatent). She also has experience with IP disputes in the Chamber for Patent and Disputes and the Russian commercial courts. Her clients include companies in media, technology, telecommunications, and many other industries.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty
Astana
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
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.

THANK YOU