Morgan Lewis

CROSS-BORDER DATA TRANSFER TRENDS: RUSSIA AND THE EU

Ksenia Andreeva
Anastasia Dergacheva
Pulina Whitaker
Brian Zimbler

February 7, 2017

Contents

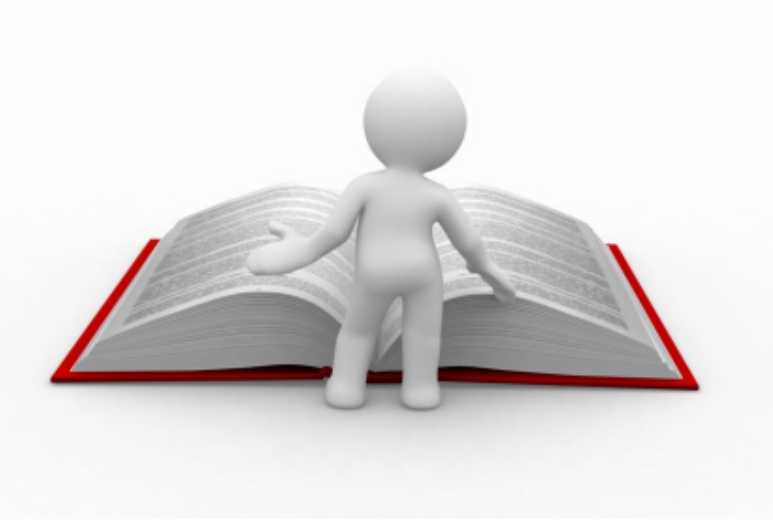
- Russia: Upcoming changes to Russian data privacy laws
- EU: Overview of the General Data Protection Regulation
- Recent regulatory practice in Russia and the EU
- Practical tips and risk mitigation strategies

SECTION 01

UPCOMING CHANGES TO RUSSIAN DATA PRIVACY LAWS

Catch-up

- Data Localization Law (Federal Law No. 242-FZ)
  - Amendments to Article 18 of Personal Data Law
  - Personal data of Russian citizens must be collected and processed using databases located in Russia
  - In force from 1 September 2015
- "Right To Be Forgotten"
  - Amendments to Information Law
  - An individual may request that search engines remove links to information that violates Russian laws, or is inaccurate, outdated or irrelevant
  - In force from 1 January 2016



New Fines for Data Processing Breaches

- Draft law No. 683952-6 approved by the Federation Council on 1 February 2017 (becomes effective on 1 July 2017)
  - Before: 1 violation (generic) with maximum fine of 10,000 Rubles (about US$167)
  - Now: 7 violations with fines up to 75,000 Rubles (about US$1270)
- How to calculate fines?
- Streamlined enforcement procedure
  - The regulator, Roskomnadzor, may directly issue notices of violation and impose fines
  - Involvement of prosecutors excluded

Other Legislative Initiatives

- Draft law No. 416052-6
  - New definition of "data processor"
  - Express provisions on electronic consent
  - Additional ground for cross-border transfer to "unqualified" countries: DTA to provide conditions for adequate protection of data subjects' rights
  - Obligation to notify any illegal disclosure of personal data
- Introduced to the State Duma in 2013, responsible committee for the 1st hearing appointed on October 6, 2016

Other Initiatives, cont'd

- Roskomnadzor has announced upcoming regulation of Big Data
  - Working group on Internet development by President's Administration to prepare draft law
  - "Big Data" to include geo-location, biometric data, user's activity on websites, etc.
  - New national operator of Big Data to be created as a state-private partnership

SECTION 02

EU: OVERVIEW OF THE GENERAL DATA PROTECTION REGULATION

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
- "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
- Pseudonymisation/anonymisation distinction
- Consent
  - explicit
  - freely given
  - fully informed

The New EU General Data Protection Regulation, cont'd

- International transfers: Binding Corporate Rules, model clauses, to certified organization, consent, transfer is "necessary" for performance of contract, establish, exercise or defend legal claims or for legitimate interests of controller (one-off and limited data subjects involved), adequate countries
- 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

The New EU General Data Protection Regulation, cont'd

- 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
- Most EU countries currently limit data protection breaches to around £500,000 per breach – average is £100,000
- 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

The New EU General Data Protection Regulation, cont'd

- 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

SECTION 03

RECENT REGULATORY PRACTICE IN RESPECT OF RUSSIAN AND EU CROSS-BORDER TRANSFERS OF PERSONAL DATA

Russia: 2016 Year in Review

- Russian personal data regulator (Roskomnadzor) statistics for Q1-Q3 2016:
  - **981** inspections and **1050** monitoring actions
  - **2162** violations
  - **464** instructions to rectify violations
  - **4.8M Rubles** in fines imposed by Roskomnadzor

- Most common violations:
  - Failure to publish/disclose privacy policy
  - Processing of data without individual's consent
  - Consent for personal data processing does not meet statutory requirements
  - Breach of confidentiality requirements
  - Processing of personal data after stated goals of processing are accomplished
  - Failure to submit notification to the regulator about processing of personal data

Case Study: LinkedIn

- Case Developments
  - May 2016: Roskomnadzor requests LinkedIn to confirm its compliance with laws
  - June 2016: Roskomnadzor files a claim to block www.Linkedin.com
  - August 2016: Court of first instance grants the claim
  - November 2016: Decision confirmed in appeal, www.LinkedIn.com blocked in Russia
- Key Takeaways
  - Russian personal data laws apply to foreign websites if the website is "directed" to Russia (based on Article 1212 of the Russian Civil Code)
  - Russian version of the website and advertising in Russian indicate that the website is "directed" to Russia
  - Domain name administrator is responsible for compliance with Russian personal data laws

Russia: Regulatory Plans for 2017

- Planned inspections, unplanned inspections, monitoring actions
- Roskomnadzor Central Federal District Department plan for 2017:
  - Telecommunication services providers
  - Consumer goods manufacturer
  - Pharmaceutical companies, hospitals
  - "Big 4" accounting firms
  - Consumer service providers, online stores
  - Banks, insurance companies, debt collection agencies
- Note: regional departments have their own plans

EU: New EU-US Privacy Shield

- To US: European Commission announced new "EU-US Privacy Shield" for US organizations in 2016, replacing the Safe Harbor programme
  - Limitations imposed on US authorities accessing personal data for national security purposes and an oversight mechanism
  - Annual review of these principles
  - EU citizens to have the same rights of enforcement as US citizens under proposed new Judicial Redress Act
  - EU citizens and EU DPAs can complain to FTC and DoC
- No equivalent for Russia which is not an "adequate" country for data exports
- Issues such as state rights of surveillance of individuals and local data protection laws applicable to EU citizens relevant for determining adequacy
- Higher standard of adequacy expected of all countries following GDPR?
- UK post-Brexit – will it still be adequate?

EU Data Transfers

- Current alternatives
  - Derogations e.g. consent to transfer outside the EU or "necessary" transfers to comply with contractual obligations or litigation management
  - Standard Contractual Clauses
  - Binding Corporate Rules
  - Assessment of adequacy
- Under the GDPR, additional options of:
  - Code of Conduct
  - Certification of mechanism and privacy seals and marks
  - Binding Corporate Rules extended to processors

EU Data Transfers: Recent Developments

- Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems – challenge to Standard Contractual Clauses between Facebook Ireland and Facebook US
- UK ICO guidance – assessment of adequacy option
- European Commission Communication – strategic framework for adequacy decisions and tools for other international data transfers

SECTION 04

FORMALIZING CROSS-BORDER TRANSFERS — PRACTICAL TIPS AND RISK MITIGATION STRATEGIES

Russia: Tips and Risk Mitigation Strategies

- Requirements for data localization
  - Purchase or lease of Russia-based server
  - Data processing agreement with local data processor
- Consent for personal data processing
  - Categories of personal data (the more, the better)
  - Precise wording (avoid "among others", "including", etc.)
  - Types of processing corresponding to stated processing goals
- Transfer of personal data
  - No recommended forms of data transfer agreements
  - Data transfer agreement = "instruction" of data operator to third party to process data by certain means and for certain purposes
  - Mutual obligations of parties to ensure confidentiality and security of data

EU: Tips and Risk Mitigation Strategies

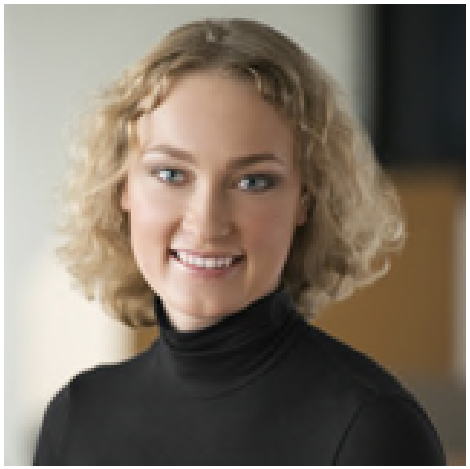
- Organisations can obtain certifications or privacy seals for data protection compliance
- Appoint a trained and sufficiently independent and senior Data Protection Officer
- Cyber and data protection liability insurance cover

Biography

Ksenia Andreeva
Moscow
T +7.495.212.2527
E 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 lawyer 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.

Biography



Anastasia Dergacheva counsels diverse clients on a variety of matters relating to intellectual property, regulatory, and antitrust matters. Anastasia represents major Russian and multinational companies in a broad spectrum of industries, including entertainment, engineering, information technologies and telecommunications industries.

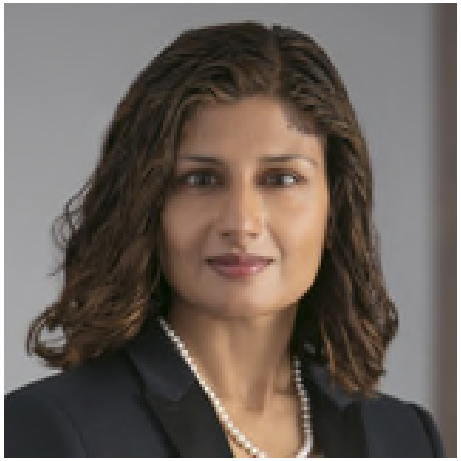
Anastasia Dergacheva

Moscow

T +7.495.212.2516

E anastasia.dergacheva@morganlewis.com

Biography



Pulina Whitaker focuses her practice on a variety of data privacy and data protection matters, including advising on international transfers of personal data, third-party transfers, data breach investigations and rights of access to personal data. She also advises on setting-up whistleblower hotlines for European-based companies and compliance with Sarbanes-Oxley Act requirements and other international investigations and compliance matters.

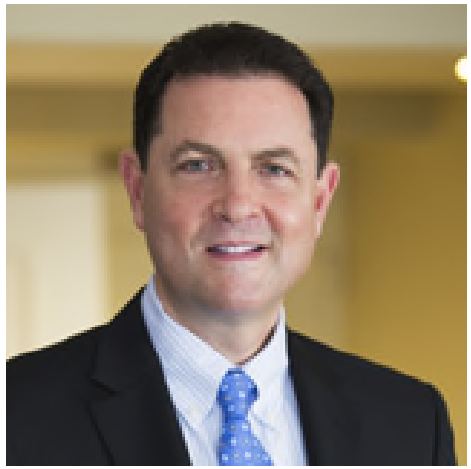
Pulina Whitaker

London

T +44.20.3201.5550

E pulina.whitaker@morganlewis.com

Biography



Brian Zimbler
Moscow/London
T +7.495.212.2511
T +44.20.3201.5552
E brian.zimbler@morganlewis.com

Brian L. Zimbler advises on cross-border investment and financial matters, primarily in emerging markets. He has more than 25 years of experience with transactions involving Russia, Kazakhstan, and other countries in the former Soviet Union. Brian serves as the Managing Partner of the Moscow office, and has advised on some of the largest foreign investments in the region. Brian represents clients in a wide range of industries, including energy, manufacturing, media, pharmaceuticals and life sciences, real property, retail, and technology.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty
Astana
Beijing
Boston
Brussels
Chicago
Dallas
Dubai
Frankfurt
Hartford
Houston
London
Los Angeles
Miami
Moscow
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Santa Monica
Shanghai
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington

Morgan Lewis

THANK YOU