
Magisters
BASED IN THE CIS
TRUSTED WORLDWIDE
www.magisters.com

Magisters

Regulatory Compliance in Data Protection: IT Aspects

AEB, Moscow, 3 June 2010

Contents

- Scope
- Legal framework
- Overview of regulatory requirements
- Licensing
- Personal data information systems
- Notification on personal data processing
- Confirmation of conformity of information systems
- Use of certified data protection software

Scope

- Focus on regulatory compliance: obligatory authorizations, notifications, certification, etc.
- Focus on issues relevant to all personal data operators / operators of automated IT systems

  - Out of scope:

  - General personal data compliance
  - Specific requirements applicable to IT companies

Health warning

- Many of the issues discussed in this presentation have not yet been tested in courts. So be careful
- It is not unlikely that certain regulatory provisions pertaining to automatic processing of personal data will be modified in the next months to come. So keep your eyes open
- Never rely on AEB presentations and always seek legal advice on your specific matter
- This presentation does not and cannot cover all issues relating to automatic personal data processing and relevant legal requirements

Legal framework

- Convention of the Counsil of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)

- Law on Personal Data (2006)
- Other Federal Laws of Russia: On Licensing of Miscellaneous Types of Activities (1998), On Information, Information Technologies and Protection of Information (2006), On Technical Regulation (2002), etc.
- Governmental regulations on licensing
- Governmental regulations on personal data processing (automatic and non-automatic)
- Resolutions of the Federal Service For Technical and Export Control, Federal Security Service and Ministry for Information Technologies and Communication on various issues related to data processing

Overview of regulatory requirements

- State license to carry out activities related to technical protection of confidential information
- Requirements applicable to automatic processing:
  - Notification to Roskomnadzor on automatic processing of personal data
  - Obligatory confirmation of conformity of personal data information systems
  - Use of certified data protection software

1.1.2011

- Grace period for bringing automated personal data information systems in compliance with the Law on Personal Data (i.e. with certification and other FSTEK requirements)
- Information systems set up after 1.1.2010 must comply now
- Does the grace period apply to IT systems that had been in existence before 1.1.2010 but were materially altered afterwards?
- Currently no enforcement

- Licensing and notification requirements: already in effect

License for technical protection of confidential information

- Art. 17 Item 11 of the Law on Licensing; Regulation On Licensing of Activities Related To Technical Protection of Confidential Information (approved by the Resolution of the Government of Russia No. 504 dated 15.8.2006)
- Activities that are subject to this licensing requirement: Measures **and/or** services for the protection of confidential information from unauthorized access or specific actions aimed at destruction or distortion of, or blocking access to such information
- The language of the regulation implies that this requirement is applicable to:
  - entities that take steps to protect confidential information for their own needs
  - entities that provide IT security services relating to protection of confidential information

License for technical protection of confidential information

- Applicability to measures for technical protection of confidential information taken for own needs:
  - Opinion of Committee for Property of the Duma: not applicable to measures taken for own needs
  - Position of regulators: the license is required even if technical protection measures are to be taken for own needs
  - Unreasonably vast scope if applied to internal data protection measures.
- Licensing conditions include: (i) the use of certified data protection software; (ii) employment of appropriate specialists; (iii) legal title to use appropriate premises, equipment and software; etc.
- The licenses for technical protection of confidential information should be applied for with the Federal Technological Service

Liability for non-compliance with the licensing requirement

- Generally, Russian law provides for administrative and criminal liability for carrying out licensable activities without the appropriate license
- Criminal liability: will likely not be applicable in case of the activities being carried out for own needs due to the condition of significant damage to third parties or significant profits derived from unlawful activities
- Administrative liability: fine in the amount of up to RUB 50,000

- Note Art. 61 of the Civil Code of Russia: possibility of liquidation in case of carrying out licensable activities without the requisite license. Highly unlikely in practice

Processing personal data

- In case of non-automated procession, no specific regulatory requirements apply (Resolution of the Government of the Russian Federation No. 687 dated 15.9.2008)

- In case of automated processing, personal data operators must obtain appropriate certifications, etc.

- Non-automated processing: all operations on personal data are controlled by humans. At the same time, information can be stored in or uploaded from an electronic database

Personal data information systems

- Personal data information system: personal information + information technologies + equipment

- Joint Order of the Federal Technical Service, the Federal Security Service and the Ministry for Information Technologies and Communication of Russia (2008): 4 classes of data protection systems depending on the volume and nature of personal data

- Class 4: no regulatory requirements
- Class 3: declaration of conformity of personal data information systems
- Classes 1 and 2: obligatory certification of personal data information systems

Notification on personal data processing

- Generally, the notification requirement is applicable to any personal data operator (Art. 22 of the Law on Personal Data)
- Notification is to be made to Roskomnadzor prior to the commencement of personal data processing

- Exceptions:

- processing personal data of employees
- processing personal data received in connection with an agreement with the personal data owner
- processing publicly available personal data or names
- non-automatic processing
- etc.

Confirmation of conformity of information systems

- Certification or declaration of conformity depending on the class of personal data system (1 and 2 – certification, 3 – declaration)
- Certain requirements must be met in order to be eligible to receive the confirmation of conformity: adoption of internal policies and other formal documents, carrying out classification of personal data system, building information protection system, etc.
- Information system must include such functions as discretionary access control, registration, integrity of trusted computing base, antivirus protection, etc. Specific requisite functions depend on the system's class and type.

- Certification is administered by the Federal Service for Technical and Export Control

Use of certified data protection software

- Data protection software that is used to protect personal data in automated personal data systems is subject to obligatory certification
- Certification of encryption software is administered by the Federal Security Service of Russia
- Certification of non-encryption data protection software is administered by the Federal Service for Technical and Export Control
- Certification of software is required in order to obtain the confirmation of conformity of personal data information system

Use of certified data protection software

- Non-encryption software: personal data certification vs. information security certification
- Possibility to certify any software that contains data protection modules or is capable of performing any data protection function
- Certification of software is a requirement on the software user, not on the software owner / distributor
- In practice, it is impossible to obtain recognition of foreign certificates
- Beware: significant time and money investment. It is recommended to purchase software that has already been certified under the FSTEK / FSB certification systems

Liability for non-compliance

- Administrative liability:

- Art. 13.12 of the Code on Administrative Offences: violation of the rules of protection of information. Fine in the amount of up to RUB 20,000
- A number of other articles of the Code on Administrative Offences providing for minor fines
- Non-certified means of data protection can be confiscated

- Compliance with data protection law can be important in civil law claims. E.g. in case of any claims being brought against a personal data operator alleging the operator's failure to provide sufficient data protection resulting in damage to third parties.

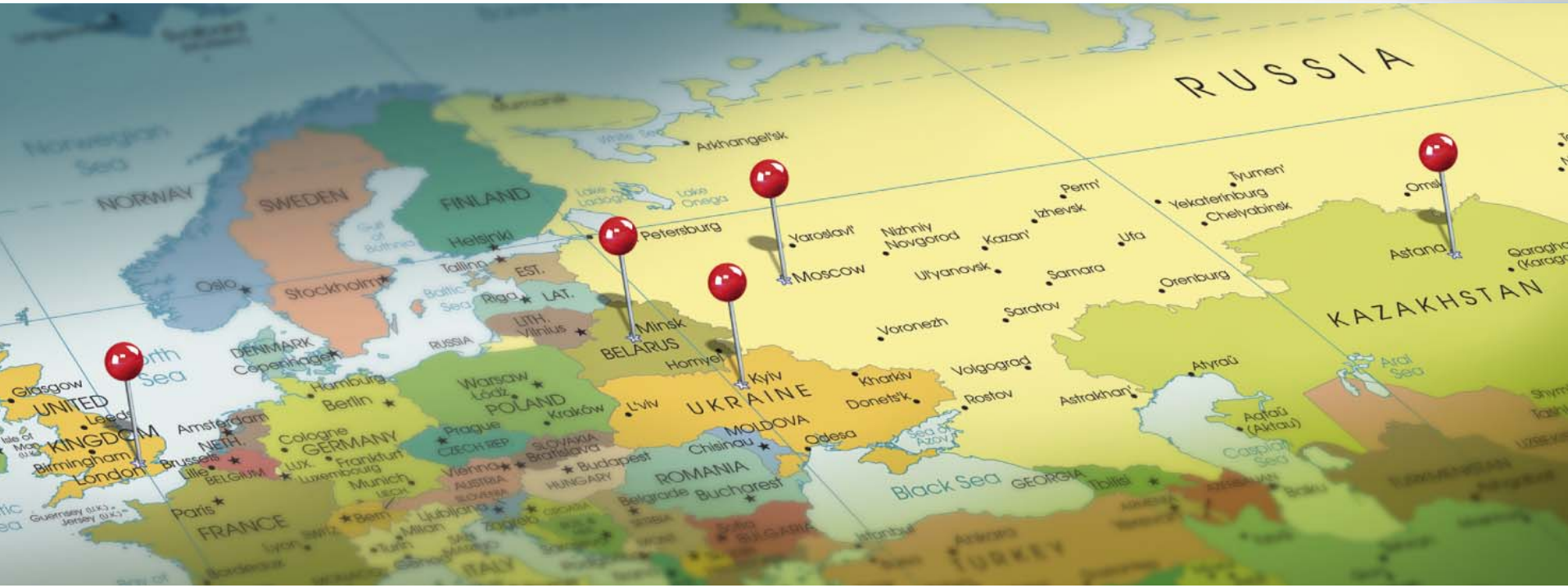
Andrey Silin

Andrey Silin, LL.M. (Konstanz)
Associate
Tel.: +7 495 730 2320
asilin@magisters.com

Focus:

- IP/IT
- M&A and corporate

About Magisters



- Offices in London, Moscow, Minsk, Kiev and Astana;
- Over 100 attorneys;
- CIS-wide Best Friends Network and Lex Mundi membership.

Thank you!

BASED IN THE CIS

TRUSTED WORLDWIDE