

# Encryption controls in Russia and the CIS

A Guest Article by Michael Vatis  
December 2008

---

---

## Encryption controls in Russia and the CIS

A Guest Article by Michael Vatis for TCii Strategic and Management Consultants

---

### Encryption licensing requirements

Encryption is a vital part of any company's information security programme. (In lay terms, "encryption" refers to data scrambling techniques to keep information secure from prying eyes and to authenticate the sender of data.) Indeed, several countries are beginning to require that sensitive information such as customers' personal information, health records and financial information be encrypted in certain situations.

At the same time, many countries strictly regulate the import, export and use of encryption. Such controls in the Russian Federation and other members of the Commonwealth of Independent States (CIS) are among the strictest in the world. These controls can complicate a company's normal communications, data storage, and information processing.

### Opening a branch office

When establishing an office in a foreign country, companies often plan to use encryption to secure the office's internal and external communications and data storage. In the Russian Federation and many other CIS countries, a company will generally need a licence to import encryption products that are designed to provide confidentiality, authentication or other services to its branch office.

Some CIS countries also require companies to obtain an additional licence for the use of encryption, including for the protection of internal communications.

### Communicating with a business partner, supplier or customer

Some companies may also wish to establish secure communications links with business partners, suppliers or customers in CIS countries. If these links utilise encryption, the company or its counterpart in the CIS may need to obtain a licence authorising the import and/or use of the encryption.

### Transferring software over the internet

Some CIS countries, including the Russian Federation, extend their licensing requirements on the import and export of encryption products to downloads and uploads of encryption software over the internet. Other countries either do not extend their rules to internet transfers as a formal matter, or don't enforce the rules in such contexts. Familiarity with local rules and practice is therefore vital to ensuring compliance and avoiding business disruption and possible penalties.

---

## Encryption controls in Russia and the CIS

A Guest Article by Michael Vatis for TCii Strategic and Management Consultants

---

### Bringing a laptop, mobile phone or PDA on a business trip

Business travellers now routinely carry laptops and other mobile devices (such as mobile phones and Blackberries) containing sensitive data. To keep such data secure, travellers often use encryption to secure data files or the entire hard drive. But here, too, encryption regulations can complicate things.

While many countries around the world have exceptions from their import restrictions for temporary imports by travellers, the Russian Federation and some other CIS countries require prior approval even for such temporary imports. Some countries have established specialised procedures for obtaining a temporary import licence, while others apply their general import licensing procedures for encryption products.

In all cases, however, travellers need to plan ahead, since any required approval process can take several weeks or more.

### Penalties

Penalties for violations of these encryption rules can be severe: they can include fines, imprisonment, or both. Violations can also result in seizure of equipment and data, causing disruption to the business.

### Conclusion

The encryption regulations in the Russian Federation and many other CIS countries create broad licensing requirements that can complicate businesses' efforts to protect their confidential information and communications.

*Michael Vatis*  
*Partner – Steptoe & Johnson LLP*

If you would like more information on any of the points covered in this Guest Article, please contact **TCii** on **020 7099 2621**.