SASMA Portal 2010

Protection of personal data- Aleksander Sanin - Leta Group

- *Aleksander Sanin*

Introduction

At first, noteworthy to say that this article was written for reference only. Any names of the companies in it are given solely to convey the current situation, although subjective in many aspects, in the Russian ITS market with regards to the personal data protection issues to the reader rather than advertise or promote them.

Now let's get back to our topic, which is the personal data protection. On January 26, 2007, the Federal Law No. 152-FZ On the personal data came into effect in Russia. Back then, virtually no one attached any importance to this event, which it gained a couple of years later.

The ITS development trends in Russia in general follow the course of the international experience and all the leading international standards are implemented in Russia although behind time. By the time the Federal Law No. 152-FZ On the personal data was passed, things used to be the way as described above – many companies brought their information security systems into compliance with ISO 17799, while others treated continuity problems and information security management seriously as guided by ISO 25999 and ISO 27001, respectively. Experts talked about the then exotic data leak prevention systems and abbreviations – DLP here and there. The information security sphere would have developed in line with the clear scenario but for the economic crisis… At this particular time as everyone still remembers the IT and ITS service markets dropped dead to zero values, while all the budgets were frozen and no one actually thought about any development of the information security industry. But this would be true subject to a small reservation – the companies still allocated funds for one very narrow objective, which was the personal data protection.

It was the personal data protection, which allowed the companies, providing information security services, to show commendable financial indices and smaller losses and sometimes even growth amidst the economic crisis. Why did that happen to the personal data? Thing is

the key fact in the personal data law was that it actually was the first statute, governing the information protection sphere, which would oblige everyone to attend to this problem. That is to say virtually every corporate body officially registered in the Russian Federation and doing any business had to comply with the Federal Law No. 152-FZ On the personal data. It was this fact, which gave a strongest incentive to the information security industry in general.

What is this "personal data protection" after all?

At first, let's tell what regulatory bodies you might have to face. The services, monitoring compliance with the laws of the personal data protection, are:

- Federal Supervision Agency for Information Technologies and Communications (this regulator is the major inspection agency)
- Federal Service for Technical and Export Control of Russia (involved in inspection wherever the examination of the personal data protection systems is implied)
- Federal Security Bureau of Russia (involved in inspection when the system is equipped with the encryption-based information safeguards)

The model inspection scheme is as follows:

The representatives of the Federal Supervision Agency for Information Technologies and Communications come to your company for whatever reason (scheduled or random check or examination). Then, they perform a standard check of your compliance with the legal requirements for the personal data protection. The inspection officers may in their sole discretion involve the representatives and experts from the Federal Service for Technical and Export Control and Federal Security Bureau.

A few words about the legal framework

If you read the Federal Law No. 152-FZ On the personal data, you should have many questions, as the law does not explain "how to protect the data?" It has a different purpose. Such things are explained by the issued and now declassified ("restricted" classification is cancelled) Guidelines of the Federal Service for Technical and Export Control of Russia and Federal Security Bureau of Russia, as well as the Enactments of the Government. Thus, at this time the following documents are the personal data protection guidelines:

- **Federal Law** No. 152-FZ On the personal data;
- **Enactment of the Government of the Russian Federation No. 781** On approval of the Regulation on the personal data protection enforcement when processed in the information systems of the personal data;
- **Enactment of the Government of the Russian Federation No. 687** On approval of the Regulation on the peculiarities of the non-automated personal data processing;
- **Order of the Federal Service for Technical and Export Control of Russia, Federal Security Bureau of Russia and Ministry of Information Technologies and Communications of Russia** No. 55/86/20 On approval of the procedures for classification of the information systems of the personal data;
- **Order of the Federal Service for Technical and Export Control of Russia as of February 5, 2010 No. 58** On approval of the Regulation on the methods and approaches to the information protection in the information systems of the personal data;
- **Resolution of the Federal Service for Technical and Export Control of Russia** as of March 5, 2010;
- **Guideline of the Federal Service for Technical and Export Control of Russia.** The basic model of the personal data security threats when processed in the information systems of the personal data;
- **Guideline of the Federal Service for Technical and Export Control of Russia**. The methods to identify the actual personal data security threats when processed in the information systems of the personal data;
- **Guideline of the Federal Security Bureau of Russia**. The recommended practice for ensuring the personal data security by means of the encryption devices when processed in the information systems of the personal data using the automation equipment;
- **Guideline of the Federal Security Bureau of Russia**. The standard requirements for arranging and ensuring performance of the cryptographic (encryption) devices designed for the protection of information, containing no data classified as state secret when used to ensure the security of the personal data when processed in the information systems of the personal data.

This is almost an exhaustive list of documents, which you will have to study, if you in good earnest decided to build an adequate personal data protection system yourself.

Today, we may say that the development of the personal data protection project is virtually the same no matter what company we speak of. It is similar from the viewpoint of a concept, while they may differ in terms of quantity (and sometimes – quality) of the reporting papers. If we split up the model personal data protection project into stages, it usually looks as follows:

- Stage 1. Inspection of the personal data processing and appraisal of the situation
- Stage 2. Development of the required organizational and management papers in the area of the personal data processing and protection
- Stage 3. Design and development of the personal data protection system
- Stage 4. Provision and implementation of the information protection devices
- Stage 5. (optional) Certification/Compliance report

This is the way a model project looks like and everyone, who has just entered this field, should clearly realize what they might meet.

In lieu of conclusion

And a few words about the Contractors, which are now operating in the market. Today, we may single out the top-5 companies in the personal data protection market in Russia:

- Jet Infosystems
- LETA
- Informzaschita
- CROC
- The fifth place is contested by several companies, such as DialogueScience, Elvis-plus and others

All the above-mentioned companies have long and well proved themselves in development of the personal data protection projects. They have dozens of successful projects. No doubt, the list of personal data protection companies and information security companies is much longer, but it wouldn't be correct or necessary to put the list of all the companies here, as it may easily

exceed 100 organizations. But, in my subjective opinion, it is better and wiser to let the well-proven professionals do this “sensitive” job, while the final choice is always done upon consideration of many factors. You should choose it after all. Dare!

Aleksander Sanin