Personal data protection in the Kyrgyz Republic

Due to technological development and the amount of information generated on a daily basis, majority of countries started to lay emphasis on the role of personal data protection and confidential information in general. Some countries adhere to the principal of data protection at the national level and limiting any kind of distribution and transfer of information. While other states believe that information is an essential factor in global economy and prosperity development, and thereby abolish restrictions on cross-border transfer of personal data.

Let's consider the data protection situation in our country. Constitution of the Kyrgyz Republic prescribes the right of every individual for personal privacy, namely it prohibits collection, storage, use and distribution of confidential and private information without the consent of the owner of such information. The Law "On information of a personal nature" No. 58 dated 14.04.2008 (the "Personal Data Law") that is aimed at legal regulation of operations with personal data was adopted in 2008. Moreover, Kyrgyzstan is a party to international agreements, according to which the legislator adopted the range of rights and obligations of personal data owner, holder, third parties and the authorized state body that guarantees data protection. However, despite the existence of the legislation in this area, in practice, it is required to adopt an effective data protection mechanism, develop a number of procedural points and establish supervisory/control mechanism that will control correspondence of personal data processing, storage and protection, establish procedure for appealing misconducts of the data holders or third parties and a system sanction for violation of the established requirements.

In our opinion, to ensure full personal data protection our state needs to focus its efforts on the three main sectors:

1) informational and educational activities for personal data subjects;

2) establishment and strengthening competence of the authorized state body on protection of personal data subjects' rights;

3) active performance of work on data protection through the authorized state body.

The lack of citizens' awareness of their rights is the main reason for systematic breach of the data protection legislation. Those who became victims of violations in the sphere of data protection often take no actions. Such failure to act results from the fact that at the present time people do not realize the danger of the personal data disclosure or do not know what actions can be taken in such cases, which authority regulates the data protection, and what guarantees should be provided by the state. Accordingly, one of the key purposes of the state should be to enhance legal literacy of the population, to promote careful attitude towards personal information as well as to increase the level of interaction between parties involved in such relations, i.e., the state, data holders and individuals. Moreover, data subjects should be aware of system violations, penalties for processing excessive data and other misconducts in the area of personal data. In order to ensure effective data protection the state should develop guidelines on conduct/management of transparent work with data, bring internal documents of data holders in compliance with the legislation requirements, develop regulations and methodology for the

proper collection, processing and storage of personal data. Personal Data Law provides for obligation of the data holder to determine a data handler for personal data processing, that should provide guarantees in respect of technical and organizational measures, governing the data processing, except cases when the data holder independently incurs functions and responsibilities of the handler onto himself/herself.[1] However, in practice, data holders do not meet this obligation due to absence of technical safety instructions that data holders must comply with while collecting, processing, storing and protecting data, as well as due to absence of the supervisory body that should regulate compliance with such measures. The legislation of the Kyrgyz Republic on data protection consists of only the Personal Data Law and the above-mentioned norm of the Constitution of the Kyrgyz Republic.

According to the Personal Data Law, an authorized state body in the sphere of data protection (the "Authorized body") which is assigned to register data holders, maintain the data holders' registry and other functions, provided by the above Law, had been established in the Kyrgyz Republic. Article 18 of the Personal Data Law prescribes that legal entities have a right to work with personal data after having completed the registration with the authorized body. The data holder and handler should provide data safety for avoidance of unlawful access, blocking, transfer, as well as an accidental or unlawful elimination, change and loss of personal data.[2]

Moreover, according to the above Law, this authorized body performs duties of a supervisory body and in cases of detecting violations or unlawful acts; subjects of personal data are allowed to file an application to the authorized state body. However, the Government of the Kyrgyz Republic had not yet adopted such body and accordingly, in practice data holders do not get registered as data holders, are not published in the data holders' registry and violations in the data protection legislation remain unpunished.

In the meantime, the Commissioner Office on protection of personal data that guarantees respect of personal data subjects' rights and conducts audits once it receives complaints had been acting in majority of European countries. Such body in the Great Britain is called the Information Commissioner's office (ICO), which is authorized to conduct audits of state bodies, individuals, as well as private sector organizations.[3] In the events of detecting violations the above body is authorized to impose fines depending on seriousness of violations or lead to criminal procedures. In the Kingdom of Belgium the Privacy Protection Commission has the above described powers, Ombudsman protecting data (Tietosuojavaltuutettu) is a supervisory body in Finland, while each federated state in Germany has its own data protecting body, which holds responsibility for compliance with the legislation in the data protection sphere.[4] The above mentioned bodies not only supervise, but also raise the legal awareness of individuals and organizations in the field of data protection, and develop technical and organizational measures to protect the data.

---

[1] Law of the Kyrgyz Republic "On information of a personal manner" 2008, No. 58, Article 17
[2] Law of the Kyrgyz Republic "On information of a personal manner" 2008, No. 58, Article 6
[3] Getting the Deal Through, "Data Protection & Privacy 2015," (London: 2015): 202
[4] DLA Piper, "Data Protection Laws of the World": 41, 132, 146

Substantial legislative changes have taken place over the past five years in other countries outside Europe, including Asia and the CIS countries. The most distinguishable changes can be seen in Singapore, where the Commission on personal data protection is established, functions of which include: development and implementation of policies and the relevant provisions in the field of personal data protection, ensuring a balance between the need to limit the collection and protection of individuals' personal data and the need of organizations to use the personal data; development of instructions for holders of personal data; examination of cases and issue of appropriate decisions and instructions; representation of the state at the international level; as well as conducting educational and outreach activities for organizations and individuals.[5] In its turn, in 2006 the Federal Law "On Personal Data" was adopted in the Russian Federation, and in 2008 the authorized body for protection of the rights of personal data subjects was formed and approved. Currently the Federal Service for Supervision of Communications Information Technology and Mass Communications is the authorized body in the Russian Federation in the sphere of protection of personal data, namely the Office for the Protection of the rights of subjects of personal data. This Office controls and supervises compliance in processing of personal data, handles complaints and appeals of citizens and legal entities on issues related to personal data processing. The Office for the Protection of the rights of the subjects conducted 805 inspections in relation to holders of personal data in 2015, during which 1188 violations were found.[6]

With daily advances and development in technology and e-commerce organizations are offered the opportunity to enter the international market and, in spite of the geographical limitations, to offer and deliver their products and services to a wide range of clients. However, in order to operate in the international market, companies need a reliable and continuous access to data, wherever that information may be. There is an opinion that there will be an impulse for the representatives of large, medium and small businesses to operate in the international market if countries do not adhere to the principle of data location, which means that the free cross-border transmission of data contributes to the economic development of each country and the world economy as a whole. This fact is the reason for this issue being raised at the international level and discussed by the business community and many countries are beginning to implement reforms in the legislation. For example, in the United States of America (the "USA") legislation does not contain any restrictions on the cross-border data transfer and allows organizations to store and move both corporate data and personal data of staff, providing adequate protection of such data. While in many European countries, cross-border transmission of data outside the European Union is prohibited, except in cases where a country provides adequate protection, or if the personal data owner had given his/her written consent to the transfer of data. In our country, as well as in the Russian Federation, the cross-border transfer of personal data is possible, if the holder of the array personal data, transmitting data, proceeds basing on the

---

[5] Personal Data Protection Commission Singapore, последнее обновление от 29.02.2016, https://www.pdpc.gov.sg/about-us/what-we-do

[6] "ComNews: На персональные данные прольется свет", the Federal Service for Supervision of Communications, Information Technology, and Mass Media, last modified November 11, 2015, https://rkn.gov.ru/press/publications/news35923.htm

existence of an international agreement between the parties, according to which the receiving party should provide an adequate level of protection of the rights and freedoms of personal data subjects and protection of personal data.[7] However, what does the "adequate level of protection" mean and who is required to determine whether a foreign state ensures an adequate level of protection of the rights and freedoms of personal data subjects? Russian practice shows that a "country that provides adequate protection" refers to countries that are parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108 dated 28.01.1981, as well as foreign countries, the list of which is approved by Roskomnadzor (the supervisory body of the Russian Federation). However, the question remains open in our country, as it is impossible to determine what level of protection is offered by any given state and in practice personal data holders independently on their own discretion determine whether a data transmission is possible. Accordingly it would be wise to include into the duties of the authorized body to determine the number of countries providing an adequate level of personal data protection and oblige personal data holders to notify in writing the authorized body on data transmission, to reflect the transfer of internal documents, in the case of the personal data owner's consent to the transfer of personal data to receive such consent in writing.

In order to ensure the protection and supervision of personal data holders' activities we believe that the Kyrgyz Republic needs to set up an authorized body or to assign responsibilities of such body to an existing institution that will control data holders in the collection, processing, storage and protection of data. Methodological recommendations on the work of such body must be developed, namely the guidelines for maintenance of the data holders register, the order of organization and carrying out state control over the collection, processing, storage and protection of the personal data, prevention and detection of violations, as well as a system of sanctions for violating the legislation in the sphere of protection of personal data. In turn, this authorized body should set public procedure of appeal of wrongful acts committed by personal data subjects, as well as a system of sanctions for violation of the established requirements. In order to ensure that activity of this body is transparent, this body should conduct annual reviews on the basis of the applicants' complaints and systemic disorders, develop and publish a strategy for further work of the body and thus ensure the stability of the overall state of the protection of the rights of personal data subjects.

[7] Zakon Kyrgyzskoi Respubliki ob informacii personalnogo haraktera [Law of the Kyrgyz Republic "On information of a personal manner"] 2008, No. 58, Article 25