Personal data security management and privacy issues of their protection in information systems

A. A. Ganiev
Z. I. Azizova, email: z.i.azizova@mail.ru

Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Аннотация. *In this article the problems of personal data protection by de-identification are discussed. The reasons for breach of confidentiality of personal data are discussed in detail, such as defining measures and means of personal data protection, minimising the costs of providing protection while complying with personal data protection requirements and others.*

Ключевые слова: *de-identification process, personal data, confidentiality, law requirements, anonymity.*

Introduction

Nowadays, much of the information related to our lives is recorded and stored digitally. Every search on any search engine, posting to a social media page, online shopping, geolocation of a mobile phone, or even a user's preferences for media content represents another recorded element of that user's dataset. The problem of personal data protection has recently been seriously exacerbated, along with changes regarding the automation of the collection and processing of socio-economic data, which has made it easier to copy, disseminate and use information of any kind, including personal data. All this has contributed to the rise of a new type of criminal activity - the illicit trafficking of personal data.

1. Security management of the personal data

The issues of information resource security are an important element in the functioning of the organisational structure in the current economic realities, which is largely due to the growing number of attacks on information systems and data repositories. With the adoption of the Republican Law of 02.07.2019 No. LRU-547 "On personal data" numerous information systems concerning the collection, storage, processing or transmission of identification data of natural persons have become subject to modernization in strict compliance with completely new requirements. The actual implementation of this law in practice will fully depend on the creation

of practical tools for its implementation and the clear formalisation of requirements for the protection of private information.

Information security of an entity means not only the ability to acquire quality information, but also the protection of already existing information from loss. Thus, according to J. Stanczy, "security is a state of trust, peace, assurance and their feeling, as well as the absence of threat and protection from danger" [1]. W. Schmid, in turn, believes that "security is a situation characterized by the absence of risk, for example, in investments, strategic plans, material assets and human resources".

There are some legal protections in place to prevent the disclosure or sale of personally identifiable information, such as name, national insurance numbers and medical records in the sale or transfer of data. However, if this data is deleted, from the small category of personally identifiable data, it can be considered anonymised. Because there is no strict regulation of anonymised data, it can be sold to anyone and used for any purpose. Once the data has been pre-cleared, it cannot be used to identify the subject and is therefore safe for later use, analysis, etc. The practice of cybercrime investigation and prevention shows that actions related to illegal copying, modification and destruction of information pose a significant threat to society and the state.

Both quantitative and qualitative changes are observed in the nature of threats, new vulnerabilities, methods and techniques of information theft are emerging. Identity theft remains a major threat. Numerous causes of information security breaches include employee negligence or the selfish and criminal intent of internal perpetrators, as well as unauthorized access and hacking of resources containing private information by an external perpetrator. Internal risks are just as dangerous as external risks. Internal perpetrators cannot be defended against as easily as malware can be defended against with an anti-virus, for example.

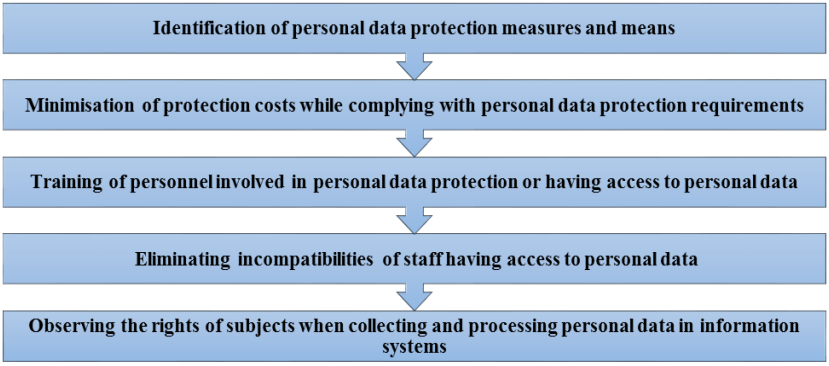
2. Security management and basic personal data protection issues

Breaches of personal data confidentiality represent a significant threat to the continuity of operations of organisations, so it seems appropriate to implement suitable policies and procedures governing the security management of the personal data being processed. This need is driven by the number and scale of the consequences of breaches of personal data security that are occurring globally. For example, in 2016 there was the theft of personal data of Yahoo users, which affected around 1 billion users, or in particular MySpace, where personal data of 427 million users was stolen. In Poland, a famous example is the disclosure of personal data of Uber users, which affected around 70,000 users. In the US, 143 million EquiFax users'

data was stolen in 2017, and in 2018 the personal data of 800,000 Swisscom customers was stolen [2].

One of the reasons for such occurrences is the low level of measures applied by the organizations to ensure the security of processed personal data. As a result, the European Union decided to radically update and amend the legislation in this field, introducing a new regulation that unifies and unifies information and personal data protection issues in all organisations in which personal data processing takes place. On 25 May 2018, the EU General Data Protection Regulation, commonly referred to as the General Data Protection Regulation (GDPR), came into force. Unfortunately, a survey conducted by ECM Insights shows that only 25% of large enterprises believe they are ready for this regulation. It should also be stressed that, according to the above-mentioned survey, almost half, i.e. as many as 45% of companies, have not yet developed a strategy to ensure compliance with the new EU requirements. Therefore, the analysis of threats in the area of information management and personal data protection in organisations as a direct result of the development of new information technologies becomes an important task. Attacks aimed at unauthorised access to private information and personal data concern all systems that operate while connected to a global network. Threats to breach the confidentiality of users' personal data can manifest themselves in a variety of ways. In addition to unauthorised access, they can also include equipment breakdowns, accidental deletion or modification by unauthorised persons.

Protection of personal data by the operator entails a number of issues implemented in figure 1.

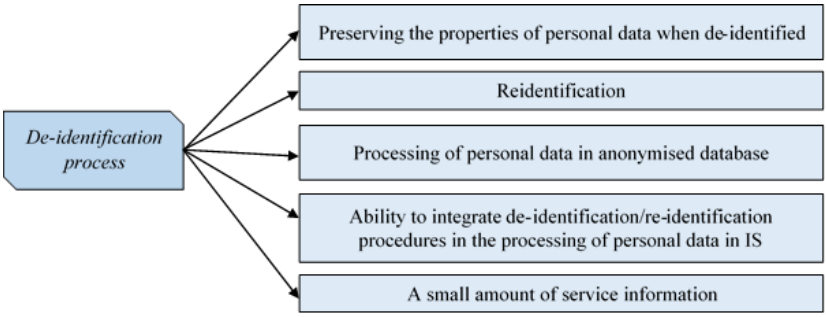


Puc. 1. Basic personal data protection issues

In accordance with the requirements of Law No. ZRU-547, the operator of the information system when processing personal data shall take the necessary legal, organisational and technical measures to protect personal data [3] from illegal or random access, destruction, modification, copying and distribution of personal data, as well as other unlawful actions. The growth in the volume of data processed creates new challenges for organisations to properly manage the personal data they hold and ensure that it is adequately protected. The information acquired and collected that can be analysed represents significant economic value.

The main rule for the personal data collection and management operator, however, should be a clear understanding of the desirability and responsibility in managing its activities.

From the set of mandatory de-identification requirements that have been formulated, the developed de-identification procedure must provide the characteristics shown in figure 2:



Puc. 2. Requirements of de-identification procedure

It means that the requirements set forth allow for the processing of de-identified data at minimum cost for upgrading existing personal data processing systems, while preserving user interfaces.

Conclusion

Thus, when design a personal data protection system, all weaknesses and vulnerabilities of personal data information systems must be taken into account, as well as the nature of possible breach targets and attacks on systems by an intruder, ways of system penetration for unauthorized access to information. The protection system should be built taking into account not only all known channels of intrusion, but also the possibility of mostly new ways of implementation of data security threats.

References

1. Współczesne pojmowanie bezpieczeństwa / Jerzy Stańczyk ; Miękka. –Używana : Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, 2011. – 355 c.

2. “Nie ma firmy za małej na bezpieczeństwo” [Электронный ресурс] : база данных. – Режим доступа : https://www.computerworld.pl/news/Nie-ma-firmy-za-malej-na-bezpieczenstwo,409986.html

3. Law of RUz No. LRU-547 of 02.07.2019. "On Personal Data". [Электронный ресурс] : база данных. – Режим доступа: https://lex.uz/docs/4396428