Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

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

A. A. Ganiev
Z. I. Azizova

Abstract:

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.

Keywords:

de-identification process, personal data, confidentiality, law requirements, anonymity.

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.

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.

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.

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

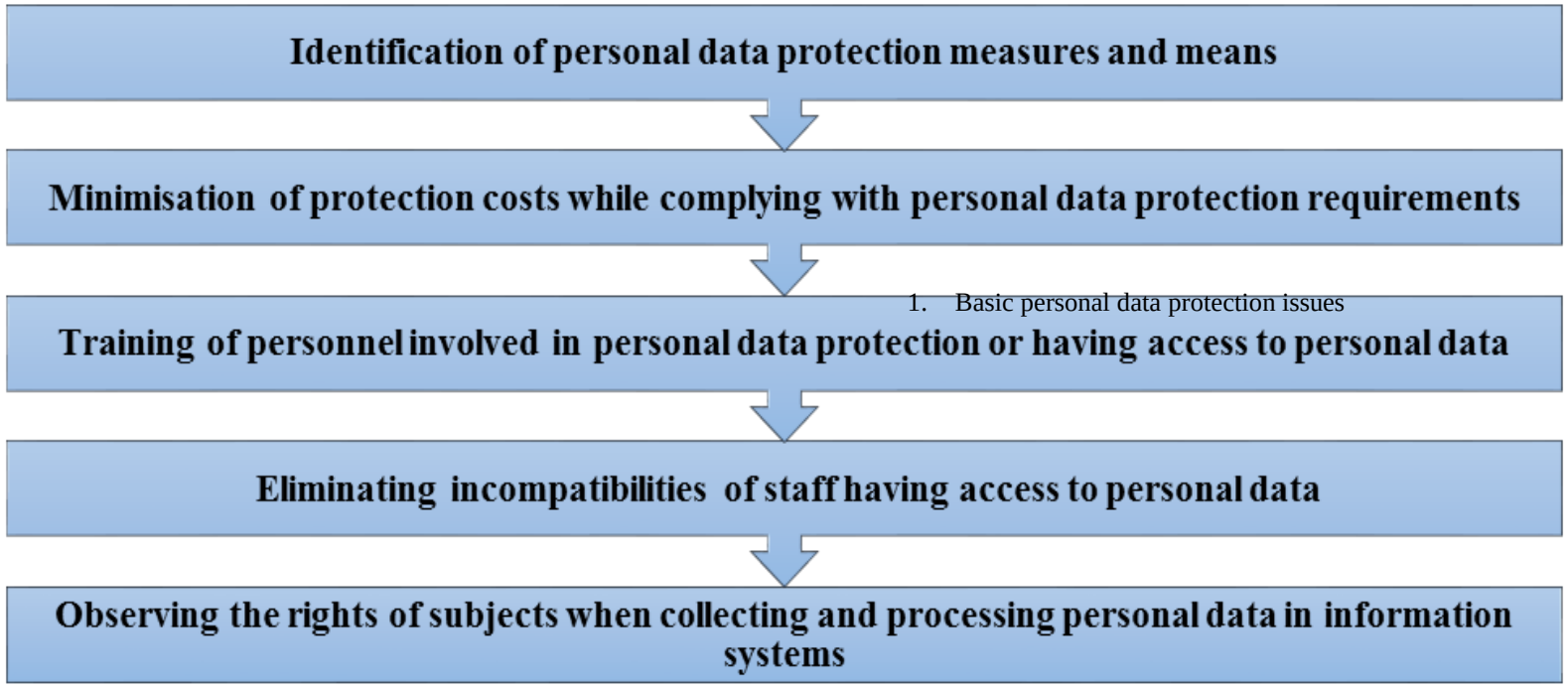

Figure 1. Basic personal data protection issues

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 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:

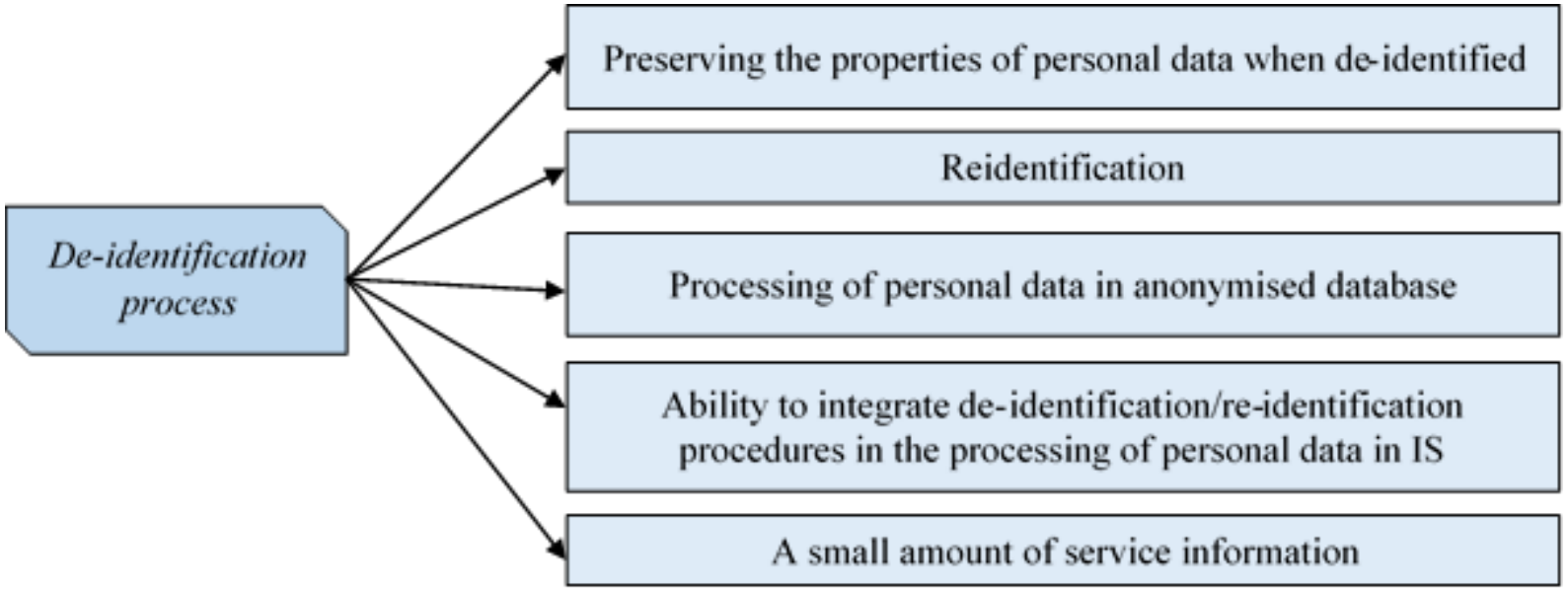

Figure 2: Requirements of de-identification procedure

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.

THANK YOU FOR ATTENTION!