



INTERNATIONAL STANDARDS FOR THE PROTECTION OF PERSONAL DATA

Author: Shahriyrov Ikrom Ibrohim o'g'li

Phone: +998 33 784-75-76

E-mail: shahriyrovikrom6@gmail.com

ARTICLE INFO:

Received: 07.10.2026

Revised: 08.10.2026

Accepted: 09.10.2026

KEY WORDS:

*personal data,
privacy, international
standards, GDPR, data
protection, legal norms,
information security,
data reliability.*

ABSTRACT

The present article will discuss the international standards of personal data protection, its importance and its legal bases. General Data Protection Regulation (GDPR) and other internationally agreed standards for ensuring the privacy and security of personal information are discussed. Special emphasis is placed on the need to harmonize these standards with the national legislation and effective implementation in practice.

Introduction

The question of what personal data is must be answered before the subject can be analyzed in detail. Personal data is defined as all information that relates to a person. Generally, there are 3 types of personal data:

- general data;
- special data;
- biometric data.

General personal data are the name, surname, personal identification numbers, passport data or personal data included in other identity documents, date and place of birth, e-mail address, place of residence, place of study and employment, family, social and property status, education, profession, income and similar data.

Telephone numbers are only considered personal information when they are written with an owner's first and last name. Vehicle registration numbers, for example, are not considered



personal data, nor are utility or housing-account numbers. This is because the first is directly related to a vehicle and the latter is related to a dwelling.

Special data are information relating to a person's racial or national origin, political, religious, and philosophical opinions, health status, intimate or private life.

Biometric data is personal data that refers to the physical and biological attributes capable of providing identification to a person. This could be anything from DNA to voice, iris, fingerprints, facial features, height, or weight.[1]

With the quick pace of digital technologies and Internet, protecting personal data is of global significance. In this aspect, many states, such as the Republic of Uzbekistan, are actively working on the creation of national laws based on international standards on the protection of personal data.

The Law of the Republic of Uzbekistan “On Personal Data” of July 02, 2019 [2] is the main law regulating the relations connected with collecting, storing, processing and protection of personal data. According to this law, “personal data” is defined as “information recorded in electronic, paper and/or tangible form related to a specific individual or enabling identification of a specific individual”. The law is also important because of its attempt to bring international standards and rules on the treatment of personal data in the country, to enhance the effectiveness of the personal data protection, to prevent any interference of the citizens constitutional rights and to protect the persons from different type of interference.[3]

Uzbekistan is making significant strides towards international standards in safeguarding human rights, such as personal data protection. The country aims to make national laws consistent with international standards to enhance digital security and ensure the privacy of citizens' lives.

Meanwhile, the modern information environment is generating novel types of violations of personal data. Hence, it is essential to deepen research on foreign experience in this area, to systematically analyze it and to apply appropriate practices to national law.

Main Part

While personal data processing might help to enhance the general information security in the future, in the immediate term, it can raise an organization's risks. The majority of people come across something or other with regard to information-security threats. For instance, they might be infected by viruses, computer worms, Trojan horses, and fraudulent software, and they might be targeted in phishing or identity theft.

Phishing is a scam designed to get confidential information, such as account information, passwords or credit-card numbers. In most cases attackers try to lure Internet users to fake sites, which can mimic the design of, for example, social networks, online stores and banks. Generally, these efforts include mass mailings of bogus e-mails with links to phishing sites that are set up to look like a legitimate organization. If a user clicks on one of these links in a web browser and enters their login credentials, they could be used to perpetrate fraud.[4]



Identity theft is a term that entered into the English language in 1964 and is defined as the use of another's personal information, including a name, bank account information, credit card or debit card number, often obtained via phishing for the purpose of fraud or other crimes. Someone whose identity is stolen for financial gain, to get loans or for any other crimes may end up being held accountable for those crimes. This may lead to serious monetary and legal consequences for the victim.

Personal privacy is also sensitive to information security, and the notion of privacy can have different meanings in different cultures. The protection of personal data is therefore one of the most pressing issues of today and it is a field in which there are many important problems that demand thorough research.

Differences in Legal Standards Across Countries

Every country has its own legislation concerning the protection of personal data. For instance, the GDPR [5] set by the European Union has stringent requirements, which differ from the Federal Privacy Act [6] and state laws in the United States. The absence of harmonisation of these systems poses challenges to global businesses.

The issue of protecting personal information is now a critical topic all over the world, and the varying requirements of different countries present a challenge to companies that do business internationally. An example is the General Data Protection Regulation (GDPR), which came into force in the European Union in 2018 and has very strict requirements for the processing of personal information. Other jurisdictions have established their own data protection laws, with companies having to meet the different laws in several jurisdictions.

Another hurdle in the international transfer of personal data is legal restrictions. For instance, the GDPR mandates that personal data can only be transferred to a country outside the EU if there is an adequate level of data-protection safeguards in place within the receiving country. This imposes some limitations on the transfer of personal data to or from countries.[7]

The Republic of Uzbekistan is also making efforts to harmonize its personal data protection system with international standards. On January 28, 2022, the “Development Strategy of New Uzbekistan for 2022-2026” was adopted which includes the implementation of international standards in the field of personal data protection, as well as in the development of the digital economy and electronic-government system.

Digital technologies and personal data security.

The risks of personal data being misused are growing with the emergence of AI, Big Data, cloud technology and the blockchain systems.

Information about cyber threats and the illegal dissemination of data.

Cybercrime and hacking are becoming more common and causing the mass disclosure and dissemination of personal information.

Lack of control over personal information by citizens.



A lot of tech giants gather the personal data of their users and then use it to market their products or services. Many activities like this are conducted without the users' awareness.

Artificial intelligence (AI) systems makes automated decisions based on information garnered and analysed about individuals. But these processes can have the potential for discrimination or poor decisions. For instance, recruitment screening tools based on AI could inadvertently discriminate against specific groups. This can lead to the issue of algorithmic discrimination.

Moreover, if transparency and accountability are lacking in automated decision-making, it can be an obstacle to making fair decisions. This may potentially result in violations of human rights. Numerous companies use the cloud as a storage solution for data. But it is not always easy to determine where these servers are and how well they are secured. This poses threats of data privacy and security.

Cloud-based services protection is especially significant in developing economies where there can be a range of issues, such as lack of legislation, less technological infrastructure and less public awareness.

In the context of the development of the Digital Economy in Uzbekistan, the need to create new technical and legal solutions to protect personal data is increasing. The digital economy is rapidly emerging, with the introduction of electronic services in the public administration and in the economic sector, and the development of the electronic-government system.

In recent years, personal details of millions of people have been leaked in the wake of cyberattacks on large corporations and government networks. An attack on the Equifax credit bureau in 2017, for instance, led to the loss of the personal data of over 147 million Americans, and such attacks may cause financial damage and privacy rights infringements as well [8].

The average person can also be a victim of cybercrime, and their personal data may be misappropriated. Phishing attacks are those that trick users into providing their financial information, logon credentials and passwords via fake sites. For instance, the users can be tricked into providing sensitive data via fraudulent messages sent by e-mail or via social networks.

Effective national measures against cyber threats in Uzbekistan should also be developed, and experience gained in other countries introduced. As cybercrime is a global phenomenon, inter-agency and international collaboration is crucial in the fight against cybercrime. Information is shared and criminals can be tracked down via cooperation with Interpol, Europol and other international agencies.

The international legal aspects of combating cybercrime are provided by international conventions, especially the Budapest Convention on Cybercrime. Uzbekistan could strengthen its global cooperation by joining this convention.[9]

Furthermore, the criminal law fight against cybercrime should be done at a national and international level. The strengthening of legal framework for prevention and fight against



cybercrime, creation of international cooperation and experience sharing are of great importance both nationally and internationally.[10]

The social threat of cybercrime is mainly related to the number of cybercrimes steadily increasing. So there is a need to understand and utilize both the national and international experience gained to prevent crimes committed in the digital environment.[11]

Besides, strengthening media literacy and information culture enables citizens to be more protected from cybercrime. Special educational programmes and training sessions should be provided for this purpose. [12]

It is also necessary to toughen up legislation against cybercrime including bank card fraud and international experience studies and implementation should be conducted.[13]

To effectively respond to cyber threats, in general, Uzbekistan needs to establish a national strategy, make use of foreign experience, and enhance citizens' information culture.

The majority of users are lacking of awareness of the way their private information is gathered, stored and utilized. This restricts them from having control over their own data. Personal data protection is not a universal right; it may be exercised taking into account the principle of proportionality in relation to other human rights.[14]

Some companies are not transparent about their collection of personal data and the purpose of that data collection. This may diminish users' trust and cause inappropriate use of information. It is important that organisations meet international standards for personal data protection and give users rights to control their personal data.[15]

The protection of personal information under the state's supervision should be tightened and transparency should be enhanced in Uzbekistan. The Law “On Personal Data” provides for the improvement of the regulatory and legal framework in the field of personal data protection.

Furthermore, the resolution on further development of the field of open data in the Republic of Uzbekistan is aimed at enhancing Uzbekistan's openness on international arena. Personal data protection is being improved by state protection measures, such as the development of digital identification systems and electronic-government services.[1]

In general, the protection of personal data can be advanced by giving users more control over their personal data, and by organisations' improved transparency.

Conclusion

In the digital world today, safeguarding personal data has become a worldwide concern. International standards – especially GDPR – offer protection for personal data and can help to prevent the misuse of it. The legislation in force in Uzbekistan should also be further developed in line with international standards for the protection of personal data. In the future, issues of information security and also individuals' control of their private data will continue to be among the most pressing issues.

In today's globalized world the protection of personal data has become an important element of the human rights. Digital technologies are being further refined and vast quantities of data are



being gathered, stored and moved. Hence, security of personal data is essential not just for upholding the right to privacy, but also for preventing personal data fraud and cybercrime.

The principles of GDPR, OECD, the ISO 27001 information-security standard, the United States Privacy Act and other international legal principles provide common guidelines for safeguarding personal data. These frameworks specifically govern how personal information is gathered, stored, processed and passed on to third parties by organizations and government institutions.

In addition, Uzbekistan is undertaking a number of reforms that will help bring its national law in line with international standards. In particular, the Law "On Personal Data" has been adopted, which regulates the protection of personal data. However, a comprehensive culture of data protection, independent supervisory authorities and institutional frameworks are needed to ensure that these norms are put into practice and make a difference.

Future protection of personal data should be reinforced with artificial intelligence, blockchain and other new technologies that are in the process of development. Meanwhile, growing international cooperation, harmonizing standards and strengthening legal and technical measures to safeguard citizens' rights will continue to be some of the key challenges for States.

References

1. G'ulom Mirzo. "Shaxsga doir ma'lumotlar himoyasi: xalqaro huquq, milliy qonunchilik va amaliy tajriba". http://nhrc.uz/oz/news/m12336#_ftn3
2. O'zbekiston Respublikasi 2019-yil 2-iyulda qabul qilingan "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni. <https://lex.uz/docs/-4396419>
3. "Shaxsga doir ma'lumotlar muhofazasi nima uchun kerak?". <https://kun.uz/26102304>
4. G'ayrat, S., & Pardayevich, Q. A. (2024). AXBOROT XAVFSIZLIGI TAMOYILLARI. JOURNAL OF INTERNATIONAL SCIENTIFIC RESEARCH, 1(2), 479-486.
5. 2018-yilda Evropa Ittifoqida qabul qilingan „Umumiy ma'lumotlarni himoya qilish qoidalari— (inglizcha: General Data Protection Regulation, GDPR)
6. AQSHda 1974-yilda qabul qilingan Federal Maxfiylik Akti – (inglizcha: Federal Privacy Act)
7. https://doctorant.tsue.uz/wpcontent/uploads/2023/06/Milliy_korporativ_boshqaruv_tizim_ini_xalqaro_standartlar_va_zamonaviy-1.pdf
8. https://www.wikiwand.com/en/articles/2017_Equifax_data_breach
9. Raimova Diyora Chori qizi. "Kiberjinoyatchilikka qarshi kurashning huquqiy jihatlari". O'qituvchi Jurnal. 5 NOYABR / 2024 YIL / 43 – SON. <file:///C:/Users/user/Downloads/Raimova+Diyora+Chori+qizi.pdf>
10. <https://cyber-law.uz/uz/subject/kiber-huquq/>
11. Toshpulatov, Akrom. (2025). RAQAMLI DUNYO SHAROITIDA SODIR
IMPACT FACTOR:13.217 **202** **IJSER.US**



ETILADIGAN JINOYATLARNING OLDINI OLISHDAGI MILLIY VA XORIJIY
TAJRIBA. https://www.researchgate.net/publication/389377416_RAQAMLI_DUNYO_SHAR_OITIDA_SODIR_ETILADIGAN_JINOYATLARNING_OLDINI_OLISHDAGI_MILLIY_VA_XORIJIY_TAJRIBA

12. Ro'ziyev Y.Z., Abdullayeva B.S. Mediasavodxonlik va axborot madaniyati: Oliy o'quv yurtlarining barcha yo'nalishlari talabalari uchun darslik. T.: O'zbekiston, 2024.

13. Abduvosit o'g'li, B. B. (2024). BANK KARTALARINI KLONLASHTIRISH UCHUN JAVOBGARLIK MASALALARI (XORIJ TAJRIBASI). Новости образования: исследование в XXI веке, 3(27), 125-129. [file:///C:/Users/user/Downloads/Bozorov+Behruzjon+Abduvosit+o%E2%80%98g%E2%80%99li+%20\(1\).pdf](file:///C:/Users/user/Downloads/Bozorov+Behruzjon+Abduvosit+o%E2%80%98g%E2%80%99li+%20(1).pdf)

14. Atanazarova Mastura Adxam Qizi (2024). SHAXSGA DOIR MA'LUMOTLARNING HIMOYA QILISHNING O'ZIGA XOS JIHATLARI.

Eurasian Journal of Law, Finance and Applied Sciences, 4 (6), 56-61. doi: 10.5281/zenodo.11560865

15. "Ma'lumotlarga egalik va foydalanuvchi huquqlari". <https://universalpublishings.com/index.php/jsiru/article/download/2902/5540/2823>

16. Ismatov Olimjon Shuxrat o'g'li. SHAXSGA DOIR MA'LUMOTLAR: XORIJIY VA MAHALLIY TAJRIBA. <https://uzmarkaz.uz/news/shaxsga-doir-malumotlar-xorijiy-va-mahalliy-tajriba>