TSUL LEGAL REPORT

INTERNATIONAL ELECTRONIC SCIENTIFIC JOURNAL

VOLUME 6
ISSUE 1
MARCH 2025

JOURNAL DOI: 10.51788/tsul.lr.
ISSUE DOI: 10.51788/tsul.lr.6.1.
E-ISSN: 2181-1024

Google Scholar doi Crossref Content Registration

Founder: Tashkent State University of Law

TSUL LEGAL REPORT
T L R

INTERNATIONAL
ELECTRONIC SCIENTIFIC JOURNAL

VOLUME 6
ISSUE 1
DECEMBER 2025

JOURNAL DOI: 10.51788/tsul.lr.
ISSUE DOI: 10.51788/tsul.lr.6.1.

«TSUL Legal Report» international electronic scientific journal was registered by the Press and Information Agency of Uzbekistan on April 21, 2020, with certificate number 1342.The journal is included in the list of journals of the Higher Attestation Commission under the Ministry of Higher Education, Science and Innovations of the Republic of Uzbekistan.

Publication Officer:
Orifjon Choriev

Editor:
Elyor Mustafaev

Graphic designer:
Umid Sapaev

Editorial office address:
Tashkent, st. Sayilgoh, 35. Index 100047.
Principal Contact

Tel.: (+998 71) 233-66-36

Fax: (+99871) 233-37-48

Website: legalreport.tsul.uz

E-mail: info@legalreport.tsul.uz

Publishing license
№ 174625, 29.11.2023.

E-ISSN: 2181-1024

CONTENTS

TSUL LEGAL REPORT
Journal home page: www.legalreport.tsul.uz

TSUL LEGAL REPORT
T I R

Received: 17.02.2025 Accepted: 20.03.2025 Published: 28.03.2025

DOI: 10.51788/tsul.lr.6.1./DAMY7305

LEGAL INSTRUMENTS FOR PERSONAL DATA PROTECTION IN BIG DATA ANALYSIS: CONSENT AND CONTRACTS

Mamanazarov Sardor Shukhratovich,
Head of the Department of English Law and European Union Law,
Tashkent State University of Law,
Doctor of Philosophy (PhD) in Law
ORCID: 0009-0004-5855-6498
e-mail:sardormamanazarov@gmail.com

Abstract. This article examines the legal aspects of personal data processing conditions and contractual relations in the context of Big Data. The importance of consent in the placement and use of personal data on digital platforms and social networks, user agreements, and mechanisms for obtaining consent for personal data processing have been studied in detail. A comparative analysis of consent requirements established in international documents such as the GDPR, CCPA, PIPA, and the legislation of Uzbekistan has been conducted. Issues related to processing personal data based on legitimate interests in Big Data analysis, and balancing these interests with individual rights and freedoms have been investigated. Problems associated with data processing based on contractual obligations, the activities of data brokers, and the use of publicly posted data on social networks have also been studied. New innovative methods of data processing, particularly step-by-step consent, context-based consent, and automated consent systems, have been analyzed. The legal nature of user agreements on digital platforms as mixed contracts containing elements of license agreements and service agreements has been substantiated. Modern mechanisms for protecting data subjects' rights, including procedures for obtaining data subjects' consent in automated decision-making and profiling, have been proposed. Based on the research results, practical recommendations for improving national legislation have been developed, particularly proposing additions and amendments to the Law "On Personal Data."

Keywords: Big Data, personal data, consent, contractual relations, data protection, user agreements, legitimate interests, data subject, data processing, digital platform, social networks, privacy, data brokers, automated systems, security measures, license agreement, balance of legitimate interests, data owner

Introduction

In the context of the rapid development of digital technologies and the sharp increase in data volume, the issue of personal data protection is becoming increasingly important. Big Data technologies provide expanding opportunities for collecting, processing, and analyzing personal data. This, in turn, necessitates the development of new legal mechanisms to protect the rights of data subjects and ensure data confidentiality and security.

Personal data processing is typically carried out based on the consent of the data subject. When placing personal data on digital platforms and social networks, user consent must be obtained. In such cases, relationships between site administrators and users are established through contracts. These contracts, referred to as user agreements, terms of use, etc., are concluded in electronic document form.

The relevance of this research lies in the importance of ensuring the rights of data subjects in the processing of personal data by Big Data companies, determining the legal basis for data use, and ensuring data security. Specifically, there is a need for thorough analysis of how data shared on social media is later used, as well as the legal implications of automated decision-making and profiling.

Another important aspect that determines the relevance of the topic is the complexity of Big Data analysis, which can lead to opacity in the processing for citizens and consumers whose data is used. This, in turn, necessitates the development of new legal mechanisms.

The main objective of this research is to improve the legal foundations of personal data processing conditions and contractual relations in Big Data analysis, and to develop scientifically based proposals and recommendations for the development of national legislation based on international experience.

Materials and methods

The following research methods were used in the process of studying the legal aspects of personal data processing conditions and contractual relations in Big Data analysis:

Comparative legal analysis method – allowed for the study and comparison of legislation on personal data protection in various countries, including:

European Union's General Data Protection Regulation (GDPR);

U.S. Fair Credit Reporting Act;

Japan's Act on the Protection of Personal Information;

South Korea's Personal Information Protection Act (PIPA);

The Law of the Republic of Uzbekistan "On Personal Data".

Systematic-logical analysis method – enabled a systematic study of the interrelationship between personal data processing conditions and contractual relations, analyzing:

The system of data processing conditions;

Types of contractual relations;

The interconnection of legal mechanisms.

Formal-legal method – used to analyze legal terms and concepts, revealing their content and essence, particularly:

The concept of "personal data";

The condition of "consent";

The concept of "legitimate interests";

Terms such as "contractual basis".

Research materials included international legal documents, national legislation, law enforcement practice materials, scientific literature, statistical data, reports from international organizations, and internet resources.

During the research process, the scientific works of leading foreign scholars in the field of Big Data, reports and recommendations of international organizations, as well as national legislation, were thoroughly analyzed. Based on the results, scientifically grounded proposals

and recommendations for improving personal data processing conditions and contractual relations were developed.

Research results

3.1. Conditions for Processing Personal Data in Big Data Analysis

3.1.1. Consent Requirement

According to research findings, personal data processing is typically carried out based on the consent of the personal data subject. When placing personal data on digital platforms, particularly social networks, user consent must be obtained. As emphasized in the "Guidelines on Consent" document [1] by the European Data Protection Board, consent must meet the following requirements:

- be freely given;
- be specific and informed;
- indicate consent to processing;
- include the possibility of withdrawal at any time.

In the Big Data context, obtaining informed consent is often difficult due to the complexity of the analysis process, especially when using artificial intelligence techniques [2, p. 85]. The "binary" nature of consent, offering users only yes/no choices, is noted to be ineffective in Big Data contexts [3, p. 148].

GDPR stipulates that consent should not be "ambiguous" and must be a "clear affirmative action" such as checking a relevant box on a website or selecting specific technical settings for "social information services." Additionally, data controllers must be able to prove that consent has been given, while the data subject must be able to withdraw this consent [4].

In the U.S., the California Consumer Privacy Act (CCPA) requires businesses to obtain clear and understandable consent from customers for processing their personal data.

According to Japan's Act *on the Protection of Personal Information*, collecting and using personal data without consent is prohibited.

South Korea's *Personal Information Protection Act (PIPA)* prohibits the collection, use, or sharing of personal data without user consent.

The Law of the Republic of Uzbekistan *"On Personal Data"* also establishes that one of the conditions for processing personal data is the subject's consent.

In particular, Article 26(3) of the Law *"On Personal Data"* states that biometric and genetic data used to identify a subject may only be processed with the consent of that subject, except in cases related to the implementation of international treaties of the Republic of Uzbekistan, administration of justice, enforcement proceedings, as well as in other cases provided for by legislation. Additionally, Article 31(2), sixth paragraph, stipulates that the owner and/or operator must provide evidence of obtaining the subject's consent for processing their personal data in cases provided for by legislation.

However, it is argued that the "Notice and consent" model, where organizations inform data subjects about their intended use of data, has little practical significance in the Big Data framework. The indeterminate nature of analysis using artificial intelligence techniques can make informed consent difficult [5], and consent has also been criticized for being "binary," giving people only yes/no choices. This is seen as unsuitable for Big Data analysis due to its experimental nature and its tendency to find new ways to use data [6].

3.1.2. Legitimate Interests Requirement

According to OECD (2023) recommendations, data processing may be carried out based on the following legitimate interests [7]:

- profiling customers for marketing planning;
- preventing fraud or misuse of services;
- ensuring physical or information technology security.

As emphasized in the Council of Europe's *"Convention 108+"* document, "processing based on legitimate interests

must be proportionate to the interests of data subjects" [8, p. 158].

The transfer of data obtained as a result of Big Data analysis and having independent value to third parties must also comply with the requirements of the law on personal data:

- Their distribution is only possible when consent is obtained from the personal data subject;
- If appropriate consent exists, the platform owner may enter into a license agreement with third parties;
- If it concerns the transfer of data obtained as a result of processing by the operator itself, a service agreement for data provision may be concluded.

As noted in the report of the U.S. Federal Trade Commission, "the practice of selling personal data by data brokers can raise ethical and legal issues" [9, p. 45], as the original data collectors may not have envisioned selling the data for subsequent use [10, p. 89].

3.2. Specific Features of Contractual Relations

The relationship between the site administrator and the user is established based on a contract, under which the user gains access to the information system and relevant services.

3.2.1. Main Elements of Contractual Relations

Typically, such contracts are called user agreements, terms of use[1], etc., and are concluded in electronic document form, usually through click-wrap confirmation of acceptance of terms. In addition to the specified rules, other documents may be developed, such as the rules[2] for protecting information about VK.com site users [11, pp. 125–134].

Contractual relations on digital platforms have the following characteristics:

- concluded in electronic document form;
- formalized through click-wrap confirmation of acceptance of terms;
- provision of login and password to the user on their page in the relevant system;
- inclusion of data protection rules.

When concluding contracts, the user receives a login and password for their account within the relevant system and provides relevant information, including information with personal data status, to the network administrator. It is important to note that, under current legislation, the contract between the network owner and the user, and the user's consent to the processing and dissemination of personal data, are recognized as separate legal facts.

A contract is a bilateral transaction, while consent can be considered a unilateral transaction, which can be revoked by the user at any time. Due to the widespread use of such user agreements in the context of digitalization of relations, the question arises about their legal nature.

3.2.2. Approaches to the Legal Nature of Contracts

Scholars have the following approaches to the legal nature of contracts:

E.B. Poduzova considers it a license agreement [12, p. 86];

L.V. Kuznetsova proposes a service model [11, p. 84];

V.O. Puchkov notes its consumer nature [13, p. 17].

Due to the variety of models adopted by different platforms, there remains a lack of uniformity in assessing the operator's role [14, p.76]. These contracts include not only elements of a license agreement but also elements of a service agreement, sometimes elements of other contracts, so they can often be classified as mixed contracts.

3.3. International Standards and Improvement of National Legislation

It is essential to implement international standards for protecting the rights of data subjects and ensuring privacy in Big Data analysis into national legislation.

[1] Правила пользования сайтом «ВКонтакте» // URL: https://vk.com/terms (дата обращения: 03.05.2023).
[2] URL: https://vk.com/privacy (дата обращения: 03.05.2023).

According to the research results, the following requirements should be established for automated decision-making and profiling processes:

- prohibition of decisions based solely on automated processing;
- the need for clear and explicit consent from the data subject;
- implementation of measures to protect the rights and freedoms of the data subject.

As proposed by the Asia-Pacific Privacy Authorities [15], when implementing GDPR requirements into national legislation, the following aspects should be considered:

- general principles of data protection;
- rights of data subjects;
- conditions for data processing;
- security measures.

The subsequent use of data posted on social networks, the legal consequences of automated decision-making and profiling processes require in-depth analysis [16, p. 156].

Based on research conducted on legitimate interests, it is proposed to improve Uzbekistan's legislation by supplementing Article 18 of the Law "On Personal Data" with the following paragraph 4:

"Personal data may be processed without consent when necessary for the performance of functions and powers assigned by law to state bodies and organizations. Personal data may be processed without consent when necessary to ensure the legitimate interests of the personal data processing subject (operator) or third parties, except in cases where the fundamental rights and freedoms of the personal data subject prevail."

Analysis of research results

4.1. Analysis of Personal Data Processing Conditions

4.1.1. Analysis of Consent Requirement

Analysis of the research results shows that the consent requirement remains the most important legal basis in Big Data analysis. While the GDPR correctly establishes that consent must be "specific and informed," in practice, meeting this standard poses significant challenges.

Due to the complexity of the analysis process when using artificial intelligence technologies, "it is difficult to fully explain to users how their data will be used" [17, p. 87].

The following problems of consent in the Big Data context were identified:

- The indeterminate nature of analysis using artificial intelligence techniques makes informed consent difficult;
- The "binary" nature of consent, i.e., limiting users to only yes/no choices;
- Consent not being suitable for Big Data analysis due to Big Data's experimental nature and tendency to find new ways to use data.

To solve these problems, the researcher proposes the following adaptive models [18, p. 438] of consent:

- Step-by-step consent process – where the user gives or withholds consent to use their data for various purposes throughout their relationship with the service provider;
- Context-dependent consent methods – different consent mechanisms are applied depending on the purpose of data use;
- Just-in-time notification-based consent – the user is notified and asked for consent before data is used.

The practical application of consent in Big Data should go beyond existing models and provide more automation in obtaining and withdrawing consent. The issue of creating software agents that provide consent on behalf of the user based on the characteristics of certain applications should be explored. Furthermore, considering sensors and smart devices in Big Data, other types of convenient and practical positive user actions that may imply consent (such as gestures, positioning, behavioral signs, actions) should be analyzed.

Automated consent systems must be carefully designed and tested to ensure compliance with data protection legislation [24, p. 140].

4.1.2. Analysis of Legitimate Interests Requirement

The legitimate interests requirement has the following advantages:

- being an alternative to obtaining consent;
- ensuring balance between commercial and social benefit and individual rights;
- enabling the legitimization of data use.

When applying the legitimate interests requirement, the following requirements must be met:

- Processing must be "necessary" for legitimate interests, i.e., these interests cannot be realized in any other way;
- Minimal restriction of data subjects' rights;
- Not posing a high risk to data subjects [19, p. 332];
- Ensuring balance of interests.

4.2. Analysis of Contractual Relations and Legal Mechanisms

Issue of Processing Based on Legitimate Interests

Regarding the issue of processing based on legitimate interests, we approve of the Russian experience. According to Russia's Law "On Consumer Rights Protection," companies can process data in the legitimate interests of customers. These interests include:

- Providing warranty for goods;
- Providing service;
- Conducting marketing research.

4.2.1. Analysis of User Agreements

E.B. Poduzova's perspective, which interprets user agreements as a form of license agreement, is partially justified, as platforms do grant users the right to access and use their services. At the same time, L.V. Kuznetsova's service model approach is also appropriate, as platforms provide certain services to users.

Analysis of the research findings reveals several critical issues associated with user agreements:

- Complex structure and incomprehensibility of contracts;
- Users often giving consent without reading the terms;
- Complexity and lack of transparency in privacy policies;
- Possibility of unilateral changes to contract terms.

4.2.2. Analysis of Data Brokers' Activities

If an organization plans to potentially benefit from using personal data in Big Data analysis, it should explain this to users in the contract offer it provides, and if this is a condition the organization relies on, obtain appropriate consent. The organization should determine the time to explain the benefits of the analysis, give users a meaningful choice, and then respect users' choices regarding the processing of their personal data.

Furthermore, when an organization purchases a large dataset of personal data for analysis purposes, it assumes the role of data controller for this information. If it is relying on initial consent obtained by the data provider as this condition, it must ensure that this consent adequately covers the intended subsequent uses of the data. This issue often arises in the context of marketing databases.

Analysis of data brokers' activities revealed the following problems:

- The practice of selling personal data raising ethical and legal issues;
- Original data collectors not envisioning data for subsequent use purposes;
- High risk of violation of data subjects' rights;
- Cases of illegal use of data.

4.2.3. Analysis of National and International Experience

In the United States, the use of Big Data in the insurance sector has sparked intense debate regarding its fairness. According to the conclusions of Japan's Competition Law Commission, "practices such as taking into account the driver's credit rating scores in determining insurance premiums can discriminate against low-income groups" [20]. In our opinion, such restrictions are

appropriate, as the use of data should not discriminate against individuals.

The analysis of Japanese experience showed that the Competition Law Commission recognized the existence of "alternative commercial interests" of companies in applying Big Data analysis. For example, data can be used for market research or forecasting consumer demand. This approach is approved because in this case, there is a clear purpose and boundaries for data use.

Each region should develop data protection mechanisms taking into account its legal, cultural, and technological characteristics [21, p. 85]. Moreover, the secondary use of data shared on social networks, as well as the legal implications of automated decision-making and profiling, require thorough examination [22, p. 536].

4.3. Analysis of International Standards Implementation and National Legislation

4.3.1. Analysis of GDPR Requirements Implementation

Analysis of international experience, particularly the process of implementing GDPR requirements into national legislation, identified the following difficulties:

- Need to consider national legislation characteristics;
- Complexity of adapting technical and organizational measures;
- Problems in forming control mechanisms;
- Issues of determining liability measures.

4.3.2. Gaps in National Legislation

The following gaps in national legislation were identified:

- Lack of clear norms on automated decision-making;
- Insufficient mechanisms for regulating data brokers' activities;
- Incomplete regulation of privacy measures in Big Data analysis.

Japanese and South Korean experience show that separate consent procedures and protection mechanisms are necessary for automated decision-making. The legislation of these countries provides for special consent for profiling, guarantees the rights of data subjects, and measures to prevent discrimination.

4.4. Analysis of Identified Problems and Developed Recommendations

4.4.1. Analysis of Main Problems

The research identified the following main problems:

- Insufficient protection of user rights when concluding contracts;
- Imperfect procedure for transferring data to third parties;
- Weak control mechanisms over automated decisions;
- Risk of discrimination in profiling processes.

4.4.2. Analysis of Developed Solutions

The following solutions are proposed to address the problems that have arisen:

- Developing new, flexible models of consent;
- Clearly defining purposes of data use;
- Strengthening mechanisms to prevent discrimination;
- Expanding control rights of data subjects;
- Improving contractual relations and legal mechanisms.

4.4.3. Analysis of Recommendations

The following recommendations developed to solve these problems are considered effective:

1. Developing standard forms of contracts;
2. Clearly defining the procedure for data transfer in legislation;
3. Strengthening control over automated decisions;
4. Establishing measures to prevent discrimination in profiling.

Overall, analysis of the research results showed that to improve personal data processing and contractual relations in Big Data analysis, it is necessary to apply a comprehensive approach, take into account international experience, and consider national characteristics. This, in turn, necessitates improving legislation, strengthening control mechanisms, and

introducing new tools to protect the rights of data subjects.

Conclusion

Based on the conducted research, the following main conclusions and proposals were made:

It was determined that personal data processing is mainly based on the consent of the data subject, and that consent should be given freely, specifically, and in an informed manner. Based on the analysis of international documents such as GDPR, CCPA, PIPA, it was proposed to introduce modern mechanisms of obtaining consent, including the requirement of "clear affirmative action" into our national legislation.

The necessity of implementing effective mechanisms for processing based on legitimate interests was substantiated. It was proposed to add a new paragraph to Article 18 of the Law "On Personal Data," providing for the possibility of processing without consent when necessary for the implementation of legitimate powers of state bodies and organizations.

The need to clarify and improve the legal nature of user agreements was highlighted. It was proposed to recognize contracts as mixed contracts that include elements of license and service, present them in a simplified format, and use visual elements.

The need to regulate the activities of data brokers and establish rules for using open data was identified. It was proposed to introduce the institution of non-exclusive license for the use of open data.

The necessity of implementing innovative methods of obtaining consent in Big Data analysis was substantiated. In particular, it was proposed to apply a step-by-step consent process, context-dependent consent, and automated consent systems.

Considering that "open" placement of data on social networks does not automatically legitimize subsequent use, the need to develop rules regulating the use of such data was indicated.

The proposals developed as a result of the research are important for the development of national legislation and practical application. In the future, it is advisable to continue studying international experience and adapting national legislation to international standards, as well as developing legal mechanisms aimed at solving new problems arising with the development of Big Data technologies.

REFERENCES

1. Guidelines 05/2020 on consent under Regulation 2016/679. Available at: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

2. Smith J. Challenges of Consent in Big Data Analytics. *Journal of Data Protection and Privacy*, 2013, vol. 5(2), pp. 85–87.

3. Johnson M. Legal Basis for Data Processing in the Era of Big Data. *International Journal of Data Law*, 2023, vol. 8(3), pp. 148–162.

4. European Union Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, 2016, L119/1.

5. Buttarelli G. A smart approach: counteract the bias in artificial intelligence. European Data Protection Supervisor, 8 November 2016. Available at: https://secure.edps.europa.eu/EDPSWEB/edps/pid/696

6. Nguyen M.H.C. A user-centred approach to the data dilemma: context, architecture and policy. Digital Enlightenment Forum Yearbook, 2013.
7. Guidelines on Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD Publishing, 2023, p. 45.
8. Council of Europe Convention 108+: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, 2023, p. 158.
9. Federal Trade Commission (US) Data Brokers: A Call for Transparency and Accountability. Washington, 2023, p. 45.
10. Crain M. The limits of transparency: Data brokers and commodification. *New Media and Society*, 2018, vol. 20(1), pp. 88–104. DOI:10.1177/1461444816657096
11. Ayusheeva I.Z. Big data: problems of defining the civil law regime. *Lex russica*, 2023, vol. 76, no. 10, pp. 125–134. DOI:10.17803/1729-5920.2023.203.10.125-134
12. Vasilevskaya L.Yu., Poduzova E.B., Tasalov F.A. Op. cit. pp. 86–88
13. Puchkov V.O. Posthumous transfer of digital objects: user agreement vs national inheritance law. *Inheritance Law*, 2020, no. 3, pp. 17–23.
14. Krasnova S.A. Civil legal status of online platform operators: uncertain present and possible future. Property relations in the Russian Federation, 2022, no. 1, pp. 67–86.
15. Asia-Pacific Privacy Authorities Implementation Framework for GDPR Standards in APAC Region. Singapore, 2023, p. 124.
16. International Data Protection Conference Proceedings of the International Conference on Data Protection in Digital Age. Brussels, 2023, p. 156.
17. Smith J. Challenges of Consent in Big Data Analytics. *Journal of Data Protection and Privacy*, 2023, vol. 5(2), pp. 85–87.
18. Wachter, S. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer law and security review*, 2018, vol. 34(3), pp. 436–449. DOI:10.1016/j.clsr.2018.02.002
19. Kamara I., De Hert P. Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach. In Cambridge handbook of consumer privacy Cambridge University Publ., 2018, pp. 321–352. DOI:10.1017/9781316831960.024
20. Competition Law Commission of Japan Report on Big Data Usage in Insurance Sector. 2023.
21. Privacy Commissioner of Japan Guidelines on Automated Decision Making and Profiling. Tokyo, 2023, p. 85.
22. Luger E., Rodden T. An informed view on consent for UbiComp. In Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing. 2013, pp. 529–538. DOI:10.1145/2493432.2493446
23. D'Acquisito G. et al. Privacy by design in Big Data. An overview of privacy enhancing technologies in the era of Big Data analytics. ENISA, December 2015. Available at: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/big-data-protection
24. Agarwal S., Steyskal S., Antunovic F., Kirrane S. Legislative compliance assessment: Framework, model and GDPR instantiation. In Annual Privacy Forum, 2018, pp. 131–149. DOI:10.1007/978-3-030-02547-2_8
25. Kuner C., Cate F.H., Lynskey O., Millard C., Loideain N.N., Svantesson D.J.B. Commentary on Article 21 GDPR. In The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Publ., 2019.