“ADOLAT”
MILLIY HUQUQIY AXBOROT MARKAZI
Guvohnoma № 636478
Litsenziya C-5669732

“HUQUQ va BURCH+” —
«ПРАВО и ДОЛГ+» —
"RIGHT and DUTY+"
Journal home page:
https://adolatmarkazi.uz/magazine/electron?id=388

2026-yil
9-son
sentabr
ISSN 3093-8546



# Legal framework for personal data protection in Uzbekistan: institutional gaps and the case for introducing the right to be forgotten

*Gavharshodbegim Norkulova,*
*Tashkent State University of Law*
*Independent Researcher*
*e-mail: gilhomova@gmail.com*

***Аннотация.*** Ushbu maqolada O‘zbekiston Respublikasida shaxsiy ma’lumotlarni himoya qilishning huquqiy asoslari, xususan 2019-yil 2-iyuldagi «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonun hamda uning 2023-yilgi yangi tahrirdagi Konstitutsiyaning 31-moddasidagi konstitutsiyaviy asosi tahlil qilinadi. Maqolada ijro etuvchi institutsional tuzilma, jumladan Davlat shaxsiylashtirish markazining Adliya vazirligi huzuridagi Shaxsiylashtirish agentligiga aylantirilishi ko‘rib chiqiladi, mavjud ma’lumot subyekti huquqlari tizimi bilan xalqaro ilg‘or amaliyot o‘rtasidagi tizimli va funksional bo‘shliqlar aniqlanadi, shuningdek Yevropa Ittifoqining Umumiy ma’lumotlarni himoya qilish reglamenti 17-moddasi va Yevropa Ittifoqi Sudining Google Spain ishi bo‘yicha amaliyoti asosida mustaqil «unutilish huquqi»ni joriy etish imkoniyati baholanadi.

***Калит сўзлар.*** shaxsiy ma’lumotlarni himoya qilish, unutilish huquqi, ma’lumotlar maxfiyligi, Umumiy ma’lumotlarni himoya qilish reglamenti, deindeksatsiya, Shaxsiylashtirish agentligi, raqamli huquqlar, ma’lumot subyekti huquqlari, axborot xavfsizligi.

***Аннотация.*** В статье рассматривается правовая база защиты персональных данных в Республике Узбекистан с акцентом на Закон «О персональных данных» № ЗРУ-547 от 2 июля 2019 года и его конституционную основу, закреплённую в статье 31 Конституции в новой редакции 2023 года. В работе анализируется институциональная архитектура, ответственная за правоприменение, включая преобразование Государственного центра персонализации в Агентство персонализации при Министерстве юстиции, выявляются структурные и функциональные пробелы между действующим режимом прав субъектов данных и международной передовой практикой, а также оценивается целесообразность введения самостоятельного права на забвение по образцу статьи 17 Общего регламента по защите данных Европейского союза и практики Суда Европейского союза по делу Google Spain.

***Ключевые слова.*** защита персональных данных, право на забвение, конфиденциальность данных, Общий регламент по защите данных,

деиндексация, Агентство персонализации, цифровые права, права субъекта данных, информационная безопасность.

***Annotation.*** This article examines the legal framework for the protection of personal data in the Republic of Uzbekistan, focusing on the Law “On Personal Data” No. ZRU-547 of 2 July 2019 and its constitutional foundation in Article 31 of the Constitution as adopted in its new edition in 2023. The article maps the institutional architecture responsible for enforcement, including the transformation of the State Personalization Center into the Personalization Agency under the Ministry of Justice, identifies structural and functional gaps between the existing data-subject rights regime and international best practice, and evaluates the feasibility of introducing a distinct right to be forgotten modelled on Article 17 of the European Union’s General Data Protection Regulation and the Google Spain jurisprudence of the Court of Justice of the European Union.

***Keywords.*** personal data protection, right to be forgotten, data privacy, General Data Protection Regulation, de-indexing, Personalization Agency, digital rights, data subject rights, information security.

***Introduction.*** The processing of personal data by public authorities, financial institutions, telecommunication operators, and private businesses has expanded rapidly in Uzbekistan over the past decade, driven by the government’s digitalisation programme and the wider Digital Uzbekistan 2030 strategy. As citizens increasingly interact with the state and with commercial actors through electronic platforms, banking applications, e-government portals, and social media, the volume of personal information collected, stored, and disseminated about identifiable individuals has grown correspondingly. This expansion has not been matched by a proportionate deepening of the data-subject rights available under domestic law. The Republic of Uzbekistan adopted its first comprehensive statute on the subject, the Law “On Personal Data” No. ZRU-547 of 2 July 2019 (hereinafter the Personal Data Law), which entered into force on 1 October 2019 and has since been amended on several occasions. [1] The Law was a significant step toward aligning Uzbek legislation with international data protection standards, yet a decade of practical application, institutional reorganisation, and comparative legal development has exposed gaps that were not apparent at the time of its adoption.

This article pursues three interconnected objectives. First, it maps the current legal and institutional framework governing personal data protection in Uzbekistan, from the constitutional guarantee introduced in the 2023 edition of the Constitution to the subordinate acts that operationalise the Personal Data Law. Second, it identifies specific institutional and normative gaps in this framework, with particular attention to the fragmentation of

regulatory competence and the absence of a coherent erasure and de-indexing mechanism. Third, it examines the case for introducing a distinct right to be forgotten into Uzbek law, drawing on the comparative experience of the European Union’s General Data Protection Regulation (GDPR) and the landmark judgment of the Court of Justice of the European Union in Google Spain, and it proposes concrete legislative measures capable of closing the identified gaps.

*Constitutional and Statutory Foundations of Personal Data Protection.* The 2023 constitutional referendum substantially strengthened the normative status of personal data protection in Uzbekistan. Article 31 of the Constitution, as adopted in its new edition, guarantees every person the right to protection of their personal data and grants individuals the right to become acquainted with information collected about them by state bodies, self-government bodies, and organisations, to correct inaccurate information, and to demand the destruction of data collected unlawfully or without legal basis. [2] This constitutional provision elevated data protection from a purely statutory matter, governed until 2023 primarily by the general privacy guarantee in Article 27 of the earlier constitutional text, to an autonomous fundamental right, thereby providing the Personal Data Law with a firmer hierarchical foundation and opening the possibility of direct constitutional review of legislation or administrative practice that infringes upon it.

At the statutory level, the Personal Data Law defines personal data broadly as information fixed on electronic, paper, or other material media that relates to an identified or identifiable natural person, and it distinguishes between the data subject, the owner of a personal data database, and the operator who carries out processing on the owner’s behalf or instruction. The Law establishes a set of data-subject rights, including the right to obtain information about the processing of one’s data, the right to demand correction of inaccurate data, and the right to withdraw consent, upon which the owner or operator is obliged to cease processing and destroy the relevant data within a statutorily defined period. Non-compliance with these obligations may trigger administrative liability under the Code on Administrative Liability and, in more serious cases, criminal liability for the unlawful collection, use, or dissemination of personal data, as introduced by the accompanying Law No. ZRU-548 of 8 July 2019 amending the Criminal Code, the Code of Criminal Procedure, and the Code on Administrative Liability. [3]

The Personal Data Law does not operate in isolation. It forms part of a broader ecosystem of information-related legislation that includes the Law “On Informatization” No. 560-II of 11 December 2003, which establishes general principles for the use of information technologies by state bodies and private actors, and the Law “On Cybersecurity” No. ZRU-764 of 15 April 2022, which imposes information-security obligations on critical infrastructure

operators, state information systems, and, to a more limited extent, private organisations processing significant volumes of data. [4] The Law "On Electronic Digital Signature" No. ZRU-793 of 12 October 2022 further underpins the legal validity of electronically executed documents and consent forms, which are increasingly the primary vehicle through which individuals authorise the processing of their personal data. [5] Sector-specific instruments, including the Law "On Bank Secrecy," the Law "On the Protection of Citizens' Health," and the Law "On Telecommunications," supplement the general regime with heightened confidentiality obligations in their respective domains.

*Institutional Architecture: Fragmentation and Overlapping Competencies.* The institutional history of personal data enforcement in Uzbekistan illustrates a pattern of repeated reorganisation rather than the development of a stable, specialised regulator. Under Article 8 of the Personal Data Law as originally enacted, the State Personalization Center under the Cabinet of Ministers was designated as the authorised state body responsible for state control over compliance with data protection legislation, the maintenance of the register of personal data databases established under Cabinet of Ministers Resolution No. 71 of 8 February 2020, and the issuance of binding instructions to eliminate violations. [6] Effective 1 January 2023, the State Personalization Center was reorganised into the Personalization Agency under the Ministry of Justice, transferring the regulator's institutional home from the executive centre of government to a sectoral ministry. [7] This reform brought data protection enforcement into closer alignment with the Ministry of Justice's broader normative and law-drafting functions, reflected in the Ministry's subsequent adoption, by orders of 15 November 2023 registered under No. 3477 and No. 3478, of Model Procedures for the processing and organisational protection of personal data within owner and operator organisations. [8]

At the same time, enforcement competence has not been consolidated exclusively within the Personalization Agency. The State Inspection for Informatization and Telecommunications has been vested with powers to monitor compliance with data localisation requirements introduced under Article 27-1 of the Personal Data Law, which mandates that databases containing the personal data of Uzbek citizens be physically located within the territory of Uzbekistan, and to maintain a separate register of infringers of data subjects' rights. The Cybersecurity Agency, established under the Law on Cybersecurity, exercises overlapping authority over the technical security of information systems that also happen to process personal data. This distribution of competence across at least three distinct bodies, the Personalization Agency, the State Inspection for Informatization and Telecommunications, and the Cybersecurity Agency, without a clear statutory delimitation of their respective jurisdictions in cases

of concurrent violation, creates uncertainty for both data subjects seeking redress and for data controllers seeking to determine the correct addressee of a compliance obligation. None of these bodies possesses the institutional independence, in terms of appointment procedure, budgetary autonomy, and insulation from ministerial direction, that is characteristic of the specialised data protection authorities established under the GDPR framework or, closer to home, discussed in ongoing reform debates within the Eurasian region.

*Existing Data-Subject Rights and the Absence of a Genuine Right to Be Forgotten.* A careful reading of the Personal Data Law reveals that Uzbek law already contains an embryonic erasure right, but one that is structurally narrower than the right to be forgotten as it has developed in comparative practice. The data subject may withdraw consent to processing at any time, in the same form in which consent was originally given, and the owner or operator is thereupon obliged to cease processing and destroy the data within a short statutorily prescribed period, generally understood in practice to be three days. [9] This mechanism, however, is entirely consent-dependent: it applies only where the original legal basis for processing was the data subject’s consent, and it provides no remedy where personal data was lawfully published, for example in a news article, a court judgment, or a public register, and continues to cause reputational or dignitary harm to the individual concerned long after its original publication ceased to serve any legitimate informational purpose. The Law also lacks any explicit provision addressing the de-indexing of personal data from search engine results, a mechanism that lies at the heart of the right to be forgotten as recognised in the European Union.

This gap is not merely theoretical. Uzbek courts and administrative bodies have, on occasion, been confronted with requests from individuals seeking the removal of outdated news items, resolved administrative proceedings, or reputationally damaging but factually accurate material from online circulation, without a clear statutory mechanism through which to balance the individual’s privacy interest against the public’s interest in access to information and the constitutionally protected freedom of the press and freedom to seek and receive information. In the absence of a dedicated right to be forgotten, such disputes are typically litigated, if at all, under the general tort provisions of the Civil Code concerning the protection of honour, dignity, and business reputation, an ill-fitting vehicle that was not designed with the specific dynamics of online information persistence and search engine indexing in mind.

*Comparative Perspectives: the GDPR and the Google Spain Doctrine.* The right to be forgotten, in its modern form, traces its origin to the judgment of the Court of Justice of the European Union in Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, in which the Court held that a

search engine operator is, under certain conditions, obliged to remove from the list of results displayed following a search on a person’s name links to web pages containing information about that person, even where the information was lawfully published and remains accurate, on the ground that the interference with the data subject’s privacy caused by continued indexing outweighs the economic interest of the operator and, in the absence of a preponderant public interest, the interest of the general public in accessing the information through that search. [10] This principle was subsequently codified in Article 17 of the GDPR, which grants the data subject the right to obtain from the controller the erasure of personal data without undue delay in defined circumstances, including where the data are no longer necessary for the purposes for which they were collected, where consent is withdrawn and no other legal basis exists, or where the data have been unlawfully processed. [11]

The GDPR model is instructive for Uzbekistan in three respects. First, it distinguishes analytically between erasure of the underlying data by the original controller and de-indexing by a search engine or intermediary, recognising that these are functionally distinct remedies addressing distinct harms, a distinction entirely absent from Uzbek law. Second, it embeds the right within a structured balancing test, requiring the controller or, upon complaint, the supervisory authority and ultimately the courts, to weigh the data subject’s interest against countervailing considerations such as freedom of expression and information, compliance with a legal obligation, public health, archiving in the public interest, and the exercise or defence of legal claims, thereby avoiding a rule so broad as to enable the suppression of legitimate matters of public record. Third, it operationalises the right through an accessible administrative complaint mechanism before an independent supervisory authority, backed by meaningful sanctioning powers, rather than relying exclusively on civil litigation. Table 1 below summarises the principal structural differences between the EU model and the current Uzbek regime.

*Institutional Gaps: Enforcement, Fragmentation, and Cross-Border Limitations***.** Beyond the substantive absence of a right to be forgotten, several structural weaknesses limit the practical effectiveness of Uzbekistan’s personal data regime as a whole. First, the fragmentation of enforcement competence described above between the Personalization Agency, the State Inspection for Informatization and Telecommunications, and the Cybersecurity Agency produces inconsistent guidance and duplicative reporting obligations for data controllers, while leaving data subjects uncertain as to which body can grant effective relief for a given category of violation. Second, none of these bodies enjoys the institutional independence associated with specialised data protection authorities elsewhere; each remains embedded within the executive hierarchy and subject to budgetary and appointment

control by a ministry or the Cabinet of Ministers, raising legitimate questions about their capacity to act against state bodies that are themselves significant processors of personal data. Third, the cross-border transfer regime under the Personal Data Law permits transfer of personal data outside Uzbekistan chiefly on the basis of the data subject's individual consent or an applicable international treaty, but Uzbekistan has not yet finalised a list of jurisdictions recognised as providing an adequate level of protection, nor has it acceded to the Council of Europe's Convention 108+, leaving businesses without a predictable adequacy or standard-contractual-clause mechanism comparable to that available under the GDPR. [12]

A further gap concerns sanctions. While the Code on Administrative Liability provides for fines in the event of unlawful processing, and the Criminal Code criminalises the most serious violations, the level of administrative fines applicable to legal entities remains modest relative to the scale of harm that large-scale data breaches or unauthorised profiling can cause, and enforcement statistics published by the Personalization Agency indicate that sanctions are applied far more frequently for formal registration failures than for substantive violations of data-subject rights such as unlawful retention or refusal to honour erasure requests. This enforcement pattern suggests that, even where the law nominally provides a remedy, the practical incentives facing controllers to comply with individual rights requests, as opposed to formal registration obligations, remain comparatively weak.

*The Case for Introducing the Right to Be Forgotten in Uzbekistan.* Three considerations support the introduction of an explicit right to be forgotten into Uzbek law. First, the constitutional foundation already exists: Article 31 of the 2023 Constitution expressly contemplates the destruction of data collected without legal basis, and a statutory right to be forgotten would give practical effect to this constitutional guarantee rather than create an entirely novel obligation. Second, the digitalisation of Uzbek media, court-decision publication practices, and administrative record-keeping means that information which was once practically obscure, dispersed across paper archives and regional newspapers, is now instantly retrievable through a simple search of an individual's name, magnifying the reputational consequences of decade-old news items, spent criminal convictions, or resolved administrative disputes in a manner the drafters of the 2019 Personal Data Law could not fully have anticipated. Third, regional and international integration considerations favour reform: as Uzbek businesses increasingly process data belonging to European data subjects or seek adequacy recognition to facilitate cross-border commerce, and as Uzbekistan considers accession to Convention 108+, aligning the domestic erasure regime with internationally recognised standards would reduce compliance friction and support the broader digital economy agenda

embodied in the Digital Uzbekistan 2030 strategy.

At the same time, any Uzbek right to be forgotten must be calibrated to avoid the principal criticism levelled against the EU model, namely the risk that a broadly framed erasure right could be invoked to suppress legitimate journalism, historical record, or matters of continuing public interest, such as the conduct of public officials or the details of financial fraud. The comparative literature on the right to be forgotten has consistently emphasised that the right is not absolute and must be embedded within a proportionality framework that gives due weight to freedom of expression and the public’s right to information. [13] An Uzbek formulation should therefore explicitly enumerate the grounds on which erasure or de-indexing may be refused, mirroring the exceptions found in Article 17(3) of the GDPR, including the exercise of the right to freedom of expression and information, compliance with a legal obligation, and the establishment, exercise, or defence of legal claims.

*Proposed Legislative and Institutional Reforms.* Based on the foregoing analysis, four reforms are proposed. First, the Personal Data Law should be amended to introduce a dedicated article, structured along the lines of Article 17 of the GDPR, establishing a right to erasure and, separately, a right to request de-indexing from search engines and content aggregators operating within Uzbekistan, subject to an explicit, enumerated set of exceptions protecting freedom of expression, legal compliance, and matters of continuing public interest. Second, the fragmented enforcement competence currently distributed across the Personalization Agency, the State Inspection for Informatization and Telecommunications, and the Cybersecurity Agency should be consolidated, or at minimum clearly delimited by inter-agency regulation, with the Personalization Agency designated as the single point of contact for data-subject rights complaints, including erasure and de-indexing requests. Third, the independence of the Personalization Agency should be strengthened through statutory guarantees regarding the appointment and removal of its leadership, protection from ministerial instruction in individual enforcement cases, and an adequately resourced budget, bringing its institutional design closer to the independent supervisory authority model that underpins the credibility of the GDPR framework. Fourth, Uzbekistan should pursue accession to the Council of Europe’s Convention 108+ and finalise the long-pending list of jurisdictions recognised as providing an adequate level of data protection, thereby providing legal certainty for the cross-border data flows on which the digital economy increasingly depends.

These reforms would not require wholesale replacement of the existing Personal Data Law, which remains, in its general architecture, consistent with recognised international principles of lawfulness, purpose limitation, and data minimisation. Rather, they

Guvohnoma № 636478 Litsenziya C-5669732 ISSN 3093-8546

represent a targeted set of amendments capable of being implemented through the ordinary legislative process, supplemented by subordinate acts of the Cabinet of Ministers and the Ministry of Justice of the kind that have already been used to operationalise other aspects of the Law, such as the 2023 Model Procedures on personal data processing.

***Conclusion.***

Uzbekistan has made substantial progress since 2019 in establishing a general legal framework for the protection of personal data, reinforced by the elevation of data protection to a constitutional right in 2023 and by a series of institutional reorganisations culminating in the creation of the Personalization Agency. Nevertheless, the analysis presented in this article demonstrates that the current framework falls short of contemporary international standards in two principal respects: it lacks a genuine right to be forgotten, encompassing both erasure and de-indexing, that extends beyond the narrow consent-withdrawal mechanism presently available, and it distributes enforcement competence across multiple institutions without the independence or procedural clarity that effective data protection requires. The comparative experience of the European Union, and in particular the doctrine developed in Google Spain and codified in Article 17 of the GDPR, offers a workable template that can be adapted to Uzbek constitutional and legal traditions without importing an unqualified or disproportionate right. The reforms proposed in this article, namely a dedicated statutory right to erasure and de-indexing subject to enumerated exceptions, consolidation and strengthening of the independence of the supervisory authority, and accession to Convention 108+, constitute a coherent and achievable legislative programme that would bring Uzbekistan’s personal data protection framework into closer alignment with international best practice while safeguarding the constitutionally protected freedoms of expression and information.

**REFERENCES:**

1. Republic of Uzbekistan. Law “On Personal Data” No. ZRU-547, July 2, 2019 (as amended). https://lex.uz/docs/4396428

2. Republic of Uzbekistan. Constitution of the Republic of Uzbekistan (new edition), adopted by nationwide referendum on April 30, 2023, in force from May 1, 2023, Art. 31. https://lex.uz/docs/6451070

3. Republic of Uzbekistan. Law “On Amendments and Additions to the Criminal Code, the Code of Criminal Procedure, and the Code on Administrative Liability of the Republic of Uzbekistan” No. ZRU-548, July 8, 2019. https://lex.uz/docs/4396429

4. Republic of Uzbekistan. Law “On Cybersecurity” No. ZRU-764, April 15, 2022. https://lex.uz/en/docs/6997403

5. Republic of Uzbekistan. Law “On Electronic Digital Signature” No. ZRU-793, October 12, 2022. https://lex.uz/en/docs/6907238

6. Cabinet of Ministers of the Republic of Uzbekistan. Resolution No. 71, February 8, 2020, “On Approval of the Regulation on the State Register of Personal Data Databases.”

7. Resolution on the reorganisation of the State Personalization Center under the Cabinet of Ministers into the Personalization Agency under the Ministry of Justice of the Republic of Uzbekistan, effective January 1, 2023.

8. Order of the Minister of Justice of the Republic of Uzbekistan No. 3478, registered November 15, 2023, “On Approval of the Standard Procedure for Processing Personal Data.”

9. Republic of Uzbekistan. Law “On Personal Data” No. ZRU-547, July 2, 2019, Art. 21.

10. Court of Justice of the European Union. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, judgment of May 13, 2014.

11. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (General Data Protection Regulation). Official Journal of the European Union, L 119/1, Art. 17.

12. Council of Europe. Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), as amended by the Protocol of 2018.

13. Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the Roots of the ‘Right to Be Forgotten’. Computer Law & Security Review, 29(3), 229–235.

14. Floridi, L. (2014). The Ethics of Memory and the Right to Be Forgotten. Philosophy & Technology, 27(3), 305–309.

15. Ambrose, M. L., & Ausloos, J. (2013). The Right to Be Forgotten Across the Pond. Journal of Information Policy, 3, 1–23.

16. Republic of Uzbekistan. Law “On Informatization” No. 560-II, December 11, 2003 (as amended). https://lex.uz/docs/4501173

17. DLA Piper. Data Protection Laws of the World: Uzbekistan. (2025). Available online.