IRSHAD Uzbek Journal of Law and Digital Policy | Volume: 4, Issue: 2
2026

Legal Regulation of Personal Data in the Republic of Uzbekistan and Conceptual Proposals for Implementing the Right to Be Forgotten

Norkulova Gavharshodbegim
Tashkent State University of Law

Abstract

This research examines the legal framework governing personal data protection in the Republic of Uzbekistan and identifies critical deficiencies in current legislation regarding individuals' rights over their digital information. The study specifically investigates the absence of a "right to be forgotten" mechanism in Uzbek law and proposes conceptual recommendations for its implementation. Employing doctrinal legal analysis and comparative methodology, the research reviews Uzbekistan's Law on Personal Data (2019) and constitutional provisions and contrasts these with the European Union's General Data Protection Regulation and other international models. The findings reveal significant legislative gaps in data subject rights, liability mechanisms, and digital governance infrastructure. The study concludes by proposing a comprehensive legislative framework for introducing the right to be forgotten in Uzbekistan, aligned with international standards while accounting for the country's unique legal, technological, and socio-economic conditions.

Keywords: Personal Data, Right to Be Forgotten, Uzbekistan Legislation, Data Protection, Digital Privacy, GDPR

APA Citation:

Gavharshodbegim, N. (2026). Legal Regulation of Personal Data in the Republic of Uzbekistan and Conceptual Proposals for Implementing the Right to Be Forgotten. *Uzbek Journal of Law and Digital Policy, 4*(2), 177–193. https://doi.org/10.59022/ujldp.593

I. Introduction

The rapid proliferation of digital technologies and the internet has fundamentally transformed how personal information is collected, stored, processed, and disseminated across the globe. In the twenty-first century, personal data has emerged as one of the most valuable commodities in the digital economy, enabling corporations, governments, and other actors to monitor, analyze, and influence individuals with unprecedented precision and scale (Mayer-Schönberger, 2009). This transformation has given rise to profound concerns about individual privacy, autonomy, and dignity, prompting lawmakers worldwide to develop new legal instruments capable of addressing the unique challenges posed by the digital environment. The tension between the free flow of information and the protection of individual privacy rights has become one of the defining legal debates of the contemporary era, with jurisdictions across the globe adopting divergent approaches to resolving this fundamental conflict. Data subjects increasingly find themselves in a position of structural vulnerability relative to large data controllers, unable to monitor the scope and nature of data processing that affects their lives.

The Republic of Uzbekistan, as a rapidly developing nation undergoing significant digital transformation, faces unique challenges in regulating personal data within its evolving legal system. Since gaining independence in 1991, Uzbekistan has undertaken substantial reforms to modernize its legislative framework, including the adoption of the Law on Personal Data in 2019, which represents the country's primary legislative instrument governing the collection, processing, and protection of personal information. The 2019 Law reflects a growing recognition within Uzbek legal and policy circles of the importance of data protection for both individual rights and economic development, particularly as the country advances its Digital Uzbekistan 2030 strategy adopted by Presidential Decree No. UP-6079 (2020). However, significant gaps remain between Uzbekistan's current legislative framework and the more comprehensive data protection regimes found in more developed jurisdictions, particularly with respect to individuals' rights to control information about themselves in the digital sphere.

One of the most significant lacunae in Uzbekistan's personal data law is the absence of a clearly defined and enforceable "right to be forgotten" the right of individuals to request the deletion or de-indexing of personal information that is no longer relevant, accurate, or necessary (Ausloos, 2012). This right, sometimes referred to as the "right to erasure," has been enshrined in the European Union's General Data Protection Regulation (GDPR) under Article 17 and recognized in various forms by courts and legislatures across Europe, Latin America, and beyond (Regulation EU 2016/679, 2016). The right to be forgotten addresses a fundamental asymmetry in the digital age: while information once published online persists virtually indefinitely, individuals change, contexts shift, and the continued availability of outdated or irrelevant personal data can cause ongoing harm to reputation, employment prospects,

and personal relationships. A criminal conviction that has been spent, a youthful indiscretion shared on social media, a medical condition disclosed without consent, or a news article based on inaccurate information all of these represent categories of personal data whose indefinite availability can cause serious and ongoing harm to the individuals concerned.

Existing scholarship on Uzbekistan's data protection regime is limited, with most academic work focusing on broader issues of internet governance, e-government development, and constitutional privacy rights rather than the specific doctrinal content of personal data law (Abdurakhmanov, 2021; Yusupov, 2020). International comparative studies of the right to be forgotten have largely focused on European, American, and East Asian jurisdictions, with post-Soviet states receiving comparatively little academic attention (Ambrose & Ausloos, 2013; Rosen, 2012). This gap in the literature means that policymakers and legal scholars in Uzbekistan lack a well-developed conceptual framework for understanding how the right to be forgotten might be adapted to the country's specific legal, cultural, and technological context. The present research seeks to address this gap by providing a systematic analysis of current legislative shortcomings and a concrete set of proposals for reform that are grounded in both international comparative experience and the particularities of the Uzbek legal system.

The central research question guiding this study is: What are the principal deficiencies in Uzbekistan's current personal data legislation with respect to individuals' rights over their digital information, and how can the right to be forgotten be effectively implemented within the Uzbek legal framework? The objectives of the study are threefold: first, to examine the existing legislative framework governing personal data protection in Uzbekistan; second, to identify specific gaps and weaknesses in current law, particularly regarding the right to be forgotten; and third, to propose conceptual recommendations for legislative reform drawing on comparative international experience. The study is significant because it addresses a pressing gap in both the academic literature and the practical policy landscape of Uzbekistan's digital governance, at a time when the country is actively pursuing legislative reform and deeper integration into the global digital economy. The findings have direct implications for legislators, legal practitioners, data protection authorities, civil society organizations, and individual citizens who seek to navigate the evolving landscape of digital rights in Uzbekistan.

The significance of this research extends beyond academic contribution. As Uzbekistan seeks to attract foreign investment, develop its digital economy, and align itself with international standards, the adequacy of its data protection regime will become an increasingly important factor in how the country is perceived by international partners, technology companies, and civil society organizations. The European Union's adequacy decision framework, which determines whether non-EU countries offer sufficient data protection to enable free data flows, provides a concrete

economic incentive for Uzbekistan to strengthen its legislation, as recognition under this framework would facilitate digital trade and data transfers with EU member states. Furthermore, the growing use of digital platforms, social media, and e-government services within Uzbekistan means that more and more citizens are affected by issues of digital privacy and data control, making legislative reform both timely and socially necessary. The right to be forgotten is not merely a technical legal construct; it reflects a broader societal commitment to human dignity, second chances, and the right of individuals to define themselves in the present rather than be permanently defined by their pasts.

II. Methodology

This study employs a qualitative research design based on doctrinal legal analysis and comparative methodology. The doctrinal approach is appropriate for this research because the primary objective is to analyze, interpret, and critically evaluate existing legal texts and identify normative gaps within Uzbekistan's personal data regulatory framework (McKenna & Bell, 2017). Comparative methodology supplements this by enabling systematic analysis of how other jurisdictions particularly the European Union, Russia, and Kazakhstan have addressed similar legislative challenges, providing a basis for informed recommendations. The study does not involve primary data collection from human participants; instead, it relies exclusively on secondary sources, including legislative texts, official regulatory documents, judicial decisions, and peer-reviewed academic literature. This methodological approach is well-established in legal scholarship and is particularly suited to the objectives of this research, which requires deep engagement with the normative content of law rather than empirical data on its application in practice.

The primary sources examined include the Constitution of the Republic of Uzbekistan (1992, as amended), the Law of the Republic of Uzbekistan “On Personal Data” No. ZRU-547 (2019), relevant presidential decrees on digital transformation, and international instruments including the Council of Europe's Convention 108+ and the UN General Assembly Resolutions on the right to privacy in the digital age. Secondary sources include peer-reviewed academic articles from legal and information technology journals, comparative law studies, and policy reports from international organizations such as the OECD, the Council of Europe, and the United Nations Special Rapporteur on Privacy. All sources were selected on the basis of relevance, credibility, and currency, with preference given to publications from the past ten years. The inclusion of both domestic and international sources reflects the inherently comparative dimension of the research, which requires simultaneous engagement with the specific content of Uzbek law and the broader international framework within which it sits. Official government and regulatory documents were accessed through official portals and verified for authenticity, while academic sources were drawn from peer-reviewed databases including Scopus, Web of Science, and

Google Scholar.

The comparative element of the methodology focuses on three primary reference frameworks: the European Union's General Data Protection Regulation (GDPR), which represents the most comprehensive international model for data protection; the Federal Law of the Russian Federation “On Personal Data” No. 152-FZ (2006, as amended), which shares legal heritage with Uzbek law through the Soviet and post-Soviet legal tradition; and the Law of the Republic of Kazakhstan “On Personal Data and Their Protection” (2013, as amended), which provides a regional comparator within the Central Asian context. By examining how these frameworks address the right to be forgotten and related rights, the study generates concrete insights applicable to the Uzbek legislative context. The analysis proceeds thematically, examining key dimensions of data subject rights, consent mechanisms, enforcement architecture, and remedial provisions.

Data analysis involves systematic content analysis of legislative texts to identify the presence, absence, or inadequacy of provisions relevant to the research objectives. A normative gap analysis framework is applied to measure the distance between current Uzbek law and international best practice standards. This framework identifies three categories of legislative gap: gaps of omission, where relevant provisions are entirely absent from current law; gaps of inadequacy, where provisions exist but are insufficiently specific, enforceable, or comprehensive to provide effective protection; and gaps of coherence, where provisions exist but conflict with or are undermined by other elements of the legal system. The findings generated through this analysis are then used to develop concrete legislative recommendations in the form of proposed statutory language, institutional design principles, and implementation guidance. The study acknowledges the limitation that it does not include empirical data on how current legislation is applied in practice, which would require a different methodological approach; this represents a fruitful area for future research that could build on the doctrinal foundations established by the present study.

III. **Results**

A. Legal Framework for Personal Data Protection in Uzbekistan

Uzbekistan's legal framework for personal data protection is anchored by the 2019 Law on Personal Data, which replaced the earlier 2009 law of the same name and represents a significant step forward in the country's data protection architecture. The 2019 Law defines personal data broadly as information recorded on material or electronic media about an identified or identifiable individual, and establishes basic principles governing data processing, including legality, purpose limitation, data minimization, accuracy, and security. The law applies to both public and private entities that collect and process personal data within Uzbekistan's territory and establishes a system of categorization distinguishing between general personal data and special categories, including biometric data and information about health,

ethnicity, and political views. An authorized body the Agency for Personal Data Protection has been established to oversee implementation and enforcement, with powers to investigate violations, issue binding instructions, and impose administrative sanctions. The 2019 Law also establishes registration requirements for databases containing personal data and prohibits cross-border transfer of personal data to countries that do not ensure an adequate level of protection.

Despite these advances, the 2019 Law contains several structural limitations that significantly constrain its effectiveness as a comprehensive data protection instrument. The law's provisions on data subject rights are relatively limited compared to international standards, granting individuals the right to access their data, request corrections of inaccurate information, and withdraw consent to processing in certain circumstances, but failing to establish a clear and enforceable right to demand deletion of personal data across digital platforms (Yusupov, 2020). The concept of a right to be forgotten understood as the right to have one's data erased from internet search results, social media platforms, and other digital repositories is not explicitly recognized in the 2019 Law, and no administrative or judicial mechanism is established to enforce such a right. This lacuna is particularly significant given the growing prevalence of digital platforms in Uzbek society and the potential for permanent online data to cause lasting reputational and professional harm to individuals. The law's provisions on consent also present limitations: while consent is identified as a lawful basis for processing, the law does not establish robust standards for the validity of consent, leaving open questions about whether consent obtained through complex terms of service agreements or in conditions of informational asymmetry satisfies legal requirements.

The enforcement framework established by the 2019 Law also presents significant challenges for effective protection. While the Agency for Personal Data Protection is empowered to investigate violations and issue sanctions, the penalty regime is modest by international standards, with administrative fines that are unlikely to deter large data controllers operating in the digital economy (Abdurakhmanov, 2021). The law does not provide for data subjects to bring private civil actions against data controllers for violations of their rights, limiting individuals' ability to seek redress through the courts independently of administrative action. Furthermore, the law contains limited provisions addressing the cross-border transfer of personal data, which is particularly relevant given the increasing use of international cloud services and social media platforms by Uzbek citizens, and the provisions that do exist lack the detailed mechanism for determining equivalence of protection that would be necessary to operationalize them effectively. The Agency for Personal Data Protection, as a relatively new institution, faces capacity constraints in terms of technical expertise, staffing, and financial resources that limit its ability to effectively monitor compliance and investigate complex violations involving sophisticated digital technologies.

B. Comparative Analysis with International Standards

The European Union's GDPR, which came into force in May 2018, represents the

global benchmark for personal data protection legislation and provides the most comprehensive legislative model for the right to be forgotten (Mantelero, 2013). Article 17 of the GDPR establishes the right to erasure as a fundamental data subject right, obligating data controllers to erase personal data without undue delay where the data subject withdraws consent, the data is no longer necessary for the purpose for which it was collected, the data subject objects to processing on grounds related to their particular situation, the data has been unlawfully processed, or there is a legal obligation to erase under Union or member state law. The GDPR also requires controllers who have made personal data public to take reasonable steps, including technical measures, to inform other controllers processing the data that the data subject has requested erasure. The GDPR's approach carefully balances the right to erasure against competing rights and interests, specifying exceptions for data processed in the exercise of the right to freedom of expression and information, for compliance with a legal obligation, for reasons of public interest in the areas of public health, for archiving purposes in the public interest, and for the establishment, exercise, or defense of legal claims.

Russia's personal data legislation provides a closer comparative model given the shared post-Soviet legal heritage between Russia and Uzbekistan. Federal Law No. 149-FZ “On Information, Information Technologies and on Information Protection” was amended in 2016 to introduce a specific right to be forgotten applicable to internet search engines, requiring them to delist search results relating to information about a natural person that is irrelevant, inaccurate, or disseminated in violation of the law. The Russian right to be forgotten is procedurally implemented through a direct request mechanism to search engine operators, who are required to process requests within ten working days and are subject to administrative fines for non-compliance. While Russia's model is narrower than the GDPR in scope applying primarily to search engines rather than all data controllers it provides a practical model for how a targeted right to be forgotten can be legislatively implemented in a civil law system similar to Uzbekistan's, without requiring the comprehensive reform of the entire data protection architecture that full GDPR alignment would demand. Kazakhstan's data protection law, amended in 2021, similarly provides for the right to request deletion of personal data in specified circumstances, though the mechanism remains less developed than either the GDPR or the Russian model and has yet to generate significant jurisprudence or enforcement activity.

The Council of Europe's modernized Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), which Uzbekistan is not currently a party to but which represents a global standard of reference, explicitly recognizes the right to erasure as a fundamental data subject right applicable where data is no longer necessary for the purpose of processing or where the legal basis for processing no longer exists. The UN Special Rapporteur on the right to privacy has similarly recognized the importance of erasure rights in the digital context, emphasizing that individuals should have effective means to require the

deletion of personal data that has been unlawfully collected or that no longer serves its original purpose. The OECD Privacy Framework, while not legally binding, also endorses principles of data quality, purpose specification, and use limitation that underpin the right to be forgotten, situating it within a broader tradition of internationally recognized privacy norms.

C. Identified Legislative Gaps in Uzbekistan

The comparative analysis reveals several critical legislative gaps in Uzbekistan's personal data framework that require systematic legislative remedy. The most fundamental gap is the absence of an explicit and enforceable right to erasure or right to be forgotten applicable across the full range of digital data controllers, including search engines, social media platforms, online news archives, and government databases. While the 2019 Law provides limited rights to withdraw consent and request correction of inaccurate data, it does not establish a general right to demand deletion of personal data that is no longer necessary, outdated, or harmful, and does not create corresponding obligations on data controllers to respond to and comply with deletion requests within defined timeframes. This gap means that Uzbek citizens who discover that harmful, outdated, or irrelevant personal information about them circulates online have no clear legal mechanism to demand its removal, leaving them exposed to ongoing reputational, professional, and personal harm without effective legal remedy.

A second critical gap concerns the territorial scope of existing legislation and its application to foreign digital platforms. The 2019 Law's jurisdictional provisions are insufficiently clear regarding its application to data controllers established outside Uzbekistan that process personal data of Uzbek citizens, creating significant uncertainty about whether major international platforms such as Google, Facebook, and YouTube are subject to Uzbek data protection law (Abdurakhmanov, 2021). This gap is particularly significant for any future right to be forgotten mechanism, since a substantial proportion of personal data about Uzbek citizens that causes reputational harm is held by foreign platforms rather than domestic data controllers. The GDPR's approach of applying to any controller that offers goods or services to EU residents or monitors their behavior regardless of establishment location represents an important legislative model that Uzbekistan could adapt to its own context. The absence of clear extraterritorial application, combined with the lack of international data protection cooperation agreements involving Uzbekistan, means that even if a domestic right to be forgotten were formally enacted, its practical enforceability against the major international platforms that most Uzbek citizens actually use would remain severely limited.

Third, the enforcement and remedial architecture of the 2019 Law is inadequate to give effect to data subject rights, even those that are formally recognized by the law. The administrative fine regime is insufficiently deterrent, with maximum fines that bear no meaningful relationship to the revenues of large digital platforms; court-based

remedies are procedurally inaccessible to most ordinary citizens due to cost, complexity, and the absence of specialized legal assistance; and there is no provision for private collective action or representative complaints by civil society organizations on behalf of affected individuals (Yusupov, 2020). By contrast, the GDPR provides for fines of up to four percent of global annual turnover for serious violations, creates rights of judicial remedy against both controllers and supervisory authorities, and enables representative actions by not-for-profit organizations mandated by data subjects, creating a multi-layered enforcement architecture that significantly enhances the practical effectiveness of the regulatory regime. The institutional capacity of the Agency for Personal Data Protection also requires strengthening: the agency currently lacks the technical expertise in digital forensics, platform auditing, and cross-border data flows that would be necessary to investigate complex violations involving major international digital platforms.

IV. Discussion

The doctrinal analysis of Uzbekistan's personal data legislation reveals a fundamental conceptual tension between the law's formal recognition of privacy as a protected value and its practical mechanisms for realizing that value in the digital context. The 2019 Law operates primarily through a consent-based model that places the burden of protection on individual data subjects, requiring them to navigate complex procedures to exercise their limited rights against well-resourced data controllers (Solove, 2013). This approach reflects a conception of privacy as a form of individual autonomy exercised through contractual consent, rather than a collective good warranting positive state intervention to ensure its effective enjoyment by all citizens. The inadequacy of the consent-based model has been extensively documented in the international literature, with scholars noting that the complexity of privacy notices, the cognitive limitations of data subjects, the ubiquity of take-it-or-leave-it terms of service agreements, and the inequality of bargaining power between individuals and large data controllers make genuine informed consent largely illusory in practice (Solove, 2013; Bennett & Raab, 2006). A legal framework that depends primarily on individual consent as the mechanism for data protection will inevitably fail to protect those who are least equipped to navigate complex digital environments often the most vulnerable members of society.

A further doctrinal problem concerns the law's narrow conception of the categories of harm that data protection is intended to prevent. The 2019 Law focuses primarily on preventing harm arising from unauthorized access, disclosure, or alteration of personal data harms associated with the traditional security paradigm of data protection but does not adequately address the harms arising from the prolonged or indefinite availability of accurate data that has become harmful through the passage of time, change of context, or the aggregation of information across multiple sources (Koops, 2011). This conception of harm fails to capture the distinctively digital phenomenon of contextual integrity violation the situation in which information

shared in one context is made permanently available in other contexts in ways that cause ongoing harm to the data subject (Nissenbaum, 2010). A right to be forgotten mechanism directly addresses this class of harm by enabling individuals to limit the temporal and contextual reach of their digital data, recognizing that information legitimately published at one time may cause unjustified harm if retained indefinitely. The law's failure to recognize this category of harm reflects a broader conceptual limitation in its approach to privacy: it treats privacy primarily as a security interest rather than as a dimension of individual autonomy and dignity that extends to the ability to control one's own narrative over time.

The absence of a right to be forgotten in Uzbek law also creates problematic incentive structures for data controllers. Without a legal obligation to delete data upon request, data controllers have strong economic incentives to retain personal data indefinitely, since data retention enables advertising targeting, user profiling, and data monetization that are central to the business models of major digital platforms (Mayer-Schönberger, 2009). The law therefore creates a structural asymmetry in which the economic interests of data controllers in data retention are implicitly privileged over individuals' privacy interests in data deletion, without any legislative mechanism for rebalancing these competing interests in favor of data subjects. This asymmetry is reflected in the disproportionate burden placed on individuals to monitor and challenge data processing rather than on data controllers to ensure ongoing necessity and proportionality of retained data. The introduction of a right to be forgotten would reverse this asymmetry by placing affirmative obligations on data controllers rather than individual data subjects to justify the ongoing retention of personal data and to honor deletion requests when those justifications no longer apply. This shift from a permissive to a more precautionary regulatory philosophy represents a fundamental change in the law's conception of the relationship between data subjects and data controllers.

The introduction of a right to be forgotten into Uzbekistan's legal system requires careful conceptual design to ensure that it effectively protects individual privacy while avoiding disproportionate restrictions on freedom of expression, access to information, and the legitimate interests of data controllers and the public. The international literature identifies three principal models for implementing the right to be forgotten: the comprehensive erasure model exemplified by Article 17 of the GDPR, applicable across all categories of data controllers; the search engine delisting model exemplified by the Google Spain decision and the Russian approach, focused narrowly on the removal of personal data from search results; and a hybrid model combining elements of both (Ambrose & Ausloos, 2013). Each model presents distinct advantages and limitations in the Uzbek context. The comprehensive erasure model offers the broadest protection but requires the most extensive reform of the regulatory architecture and the greatest institutional capacity to implement effectively. The search engine delisting model is more limited in scope but is practically achievable with existing institutional resources and provides a meaningful remedy for one of the most

common and impactful forms of digital privacy harm. A hybrid model, which begins with targeted search engine delisting but provides a pathway for progressive extension of erasure rights across other categories of data controllers, offers the most pragmatic approach for a jurisdiction at Uzbekistan's stage of data protection development.

A foundational principle for any Uzbek right to be forgotten must be the proportionality of the right against competing interests, particularly the right to freedom of expression and access to information. The right to be forgotten has attracted criticism from some academic and journalistic quarters as potentially threatening press freedom and the public's right to access information, particularly where it is invoked to suppress reporting on matters of genuine public interest (Rosen, 2012). These concerns are legitimate and must be taken seriously in legislative design, particularly given Uzbekistan's commitments under the International Covenant on Civil and Political Rights and its own constitutional guarantee of freedom of speech and press. The GDPR's approach of specifying exceptions to the right to erasure for data processed for journalistic, scientific, historical, and research purposes, as well as for data processed for the establishment, exercise, or defense of legal claims, provides a useful template for balancing these competing interests. Any Uzbek implementation should incorporate robust exceptions for public interest expression, defining these exceptions with sufficient clarity to prevent their abuse by data controllers seeking to circumvent erasure obligations while ensuring that genuine journalism and public interest research are protected. The design of these exceptions will require careful legislative drafting and ultimately judicial interpretation to determine their appropriate scope in specific cases.

The triggering conditions for the proposed right to be forgotten should be defined with precision to ensure that the right operates effectively in the specific categories of cases where the harm from continued data availability is most clearly established. Drawing on international models and adapting them to the Uzbek context, this research proposes the following triggering conditions: first, where the personal data is no longer necessary in relation to the purposes for which it was collected or processed; second, where the data subject withdraws consent and there is no other legal ground for processing; third, where the data has been unlawfully processed, including data obtained through breach of confidentiality, unauthorized access, or deception; fourth, where the data concerns matters for which the data subject has completed a legal penalty or rehabilitation period, particularly relevant for criminal records and judicial proceedings; fifth, where the data concerns a natural person who was a minor at the time of collection and whose interests are no longer served by its continued availability; and sixth, where the continued availability of the data causes disproportionate harm to the data subject relative to any legitimate interest served by its retention (Koops, 2011). Each of these conditions reflects a specific category of harm arising from digital data retention, and together they define a principled and practically workable scope for the right to be forgotten in the Uzbek context.

To give effective legal expression to the right to be forgotten in Uzbekistan, several concrete legislative mechanisms are proposed, each addressing a specific dimension of the regulatory gap identified in the preceding analysis. First, the 2019 Law on Personal Data should be amended to explicitly recognize the right to erasure as a fundamental data subject right, defined in terms that encompass both the deletion of data from data controllers' systems and the de-indexing of data from search engine results. The amended provision should specify the triggering conditions for the right, the procedure for submitting erasure requests to data controllers, and the timeframe within which data controllers are obligated to respond proposed as thirty calendar days, consistent with GDPR standards with provisions for extensions of up to a further sixty days in cases of particular complexity or volume. Data controllers should be required not only to delete the data from their own systems but also to communicate the erasure request to any third parties to whom the data has been disclosed, and to make reasonable technical efforts to inform other controllers of the request where the data has been made public. The law should also establish a right for data subjects to receive confirmation of erasure, providing assurance that their request has been honored and creating an evidentiary basis for any subsequent enforcement action.

Second, a new dedicated provision should be introduced specifically addressing the right to de-indexing, applicable to search engine operators and online content aggregators operating in or accessible from the territory of Uzbekistan. This provision should require search engine operators to remove from their search results links to web pages containing personal data about a natural person that is irrelevant, outdated, inaccurate, or disseminated in violation of applicable law, upon a reasoned written request from the data subject. The provision should establish clear procedural requirements for processing such requests, including mandatory acknowledgment within five working days, substantive assessment and decision within thirty days, and a duty to provide written reasons for any refusal that can be appealed. Search engine operators should be required to provide clear, accessible, and free mechanisms for submitting de-indexing requests, analogous to the forms currently made available by Google and other major search engines in response to GDPR requirements. The provision should also establish an obligation for search engine operators to maintain records of requests received, decisions taken, and the grounds for refusals, to enable oversight by the Agency for Personal Data Protection and to facilitate the development of consistent decision-making standards over time.

Third, the enforcement framework of the 2019 Law must be substantially strengthened to ensure that the right to be forgotten is practically enforceable rather than merely nominal. The administrative fine regime should be revised upward to create genuine deterrence against non-compliance, with fines calibrated by reference to the seriousness of the violation, the size and financial resources of the data controller, the duration of non-compliance, and the number of data subjects affected. For the largest digital platforms, fines should be calculated as a percentage of annual global turnover the GDPR's model of up to four percent provides an appropriate

benchmark to ensure that penalties bear a meaningful relationship to the scale of the controller's operations and the economic benefit derived from the retained data. A private right of action should be introduced enabling data subjects to bring civil claims for compensation for material and non-material damage suffered as a result of violations of their erasure rights, providing an additional layer of accountability that supplements administrative enforcement. The Agency for Personal Data Protection should be empowered to conduct audits of data controllers' processing activities on its own initiative, to accept and investigate complaints from data subjects and civil society organizations, and to take urgent interim measures including ordering temporary suspension of data processing where evidence of serious ongoing violations is established.

Fourth, the extraterritorial application of Uzbekistan's data protection law should be explicitly extended to cover foreign data controllers that process personal data of Uzbek citizens in the context of offering goods or services in Uzbekistan or monitoring the behavior of persons within Uzbekistan, regardless of where the controller is established. This extension is essential to ensure that the right to be forgotten can be effectively invoked against the major international platforms that control most of the digital data about Uzbek citizens. The law should include provisions for cooperation with foreign data protection authorities and for the negotiation of bilateral and multilateral data protection agreements with key partner countries, following the model of the EU's adequacy framework and the APEC Cross-Border Privacy Rules system. Uzbekistan should also consider seeking association with the Council of Europe's Convention, which would provide access to an established international network of data protection cooperation and would signal the country's commitment to internationally recognized privacy standards. Pursuing these international dimensions of reform in parallel with domestic legislative changes would maximize the practical impact of the right to be forgotten and embed it within a sustainable framework of international data governance.

The successful implementation of a right to be forgotten in Uzbekistan will face several practical challenges that must be anticipated and addressed in the legislative design and accompanying policy measures. The first and most fundamental challenge is institutional: effective implementation requires that the Agency for Personal Data Protection develop the technical capacity to evaluate erasure requests, monitor compliance by digital platforms, and investigate violations involving complex cross-platform data flows. International experience with GDPR implementation suggests that regulatory agencies require substantial investment in digital forensics, data science expertise, and international regulatory networks to discharge these functions effectively (Bennett & Raab, 2006). Uzbekistan should prioritize capacity-building within the Agency through targeted recruitment of technical specialists, investment in digital investigation tools, and active participation in international regulatory cooperation networks. The establishment of a dedicated digital rights unit within the Agency, with specific responsibility for processing erasure complaints and monitoring

compliance by major digital platforms, would help ensure that the new right is administered by personnel with the appropriate technical and legal expertise.

A second significant challenge concerns legal culture and awareness among both data controllers and data subjects. The effectiveness of the right to be forgotten depends not only on the formal legal framework but on the practical knowledge and willingness of individuals to exercise their rights and of data controllers to comply with their obligations. Survey evidence from EU member states implementing the GDPR suggests that many individuals remain unaware of their data rights despite significant public information campaigns, and that compliance by data controllers, particularly small and medium-sized enterprises, is often incomplete (Mantelero, 2013). Uzbekistan should invest in comprehensive public education campaigns explaining the right to be forgotten, the circumstances in which it can be invoked, and the procedures for submitting requests, delivered through multiple channels including social media, school curricula, and community outreach programs. Civil society organizations, including consumer protection groups and digital rights advocates, should be actively engaged and funded as partners in promoting rights awareness and providing practical assistance to individuals seeking to exercise their rights. Compliance guidance for data controllers, developed in consultation with industry representatives and published in accessible language, would help reduce the compliance burden on smaller entities while raising standards across the sector.

A third challenge relates to the tension between the right to be forgotten and Uzbekistan's obligations under international law regarding freedom of expression and access to information. Article 19 of the International Covenant on Civil and Political Rights, to which Uzbekistan is a party, guarantees the right to freedom of expression including the freedom to seek, receive, and impart information, and any restriction on this right must be necessary and proportionate. A poorly designed or overly broad right to be forgotten could potentially be used to suppress legitimate journalism, historical documentation, or accountability reporting, undermining these fundamental commitments. Legislative design should therefore include robust safeguards for journalism and public interest expression, including a clearly articulated exception for data processed in the public interest or for the purposes of scientific or historical research, and a requirement that refusals of erasure requests on grounds of freedom of expression be clearly reasoned and subject to independent review by the Agency for Personal Data Protection and the courts. The Agency should develop guidance on the balance between the right to be forgotten and freedom of expression, drawing on the jurisprudence of the European Court of Human Rights and the European Court of Justice, adapted to the specific legal and cultural context of Uzbekistan.

The introduction of a right to be forgotten would have broader implications for Uzbekistan's digital governance framework that extend beyond the specific context of personal data law. It would signal a commitment to aligning Uzbekistan's legal system with international standards of digital rights protection, potentially facilitating the

country's eventual recognition under the EU's adequacy framework and enhancing its attractiveness as a destination for digital investment and technology partnerships. Such recognition would have concrete economic benefits, enabling the free flow of personal data between Uzbekistan and EU member states and facilitating the operations of European companies doing business in Uzbekistan. The right to be forgotten also sits within a broader ecosystem of digital rights including data portability, algorithmic transparency, and protection against automated decision-making that Uzbekistan will need to develop progressively as its digital economy matures. Early legislative action in this area would position Uzbekistan favorably for future regulatory developments and demonstrate a proactive rather than reactive approach to digital governance that international partners and investors would view positively.

The right to be forgotten also intersects with Uzbekistan's developing cybersecurity and information security legal frameworks, since effective implementation requires robust mechanisms for data breach notification, incident response, and cross-platform data management. Legislative reform in the personal data field should be carefully coordinated with parallel developments in cybersecurity law to ensure coherence and avoid gaps or conflicts between different regulatory regimes governing the security and integrity of digital information. The Agency for Personal Data Protection should work closely with the State Inspectorate in the field of information technologies, the Committee for the Development of Information Technologies and Communications Industry, and other relevant government bodies to develop integrated approaches to digital rights protection that address both the privacy and security dimensions of personal data governance. The establishment of a formal inter-agency coordination mechanism for digital rights issues, with regular meetings, shared information systems, and joint enforcement protocols, would help ensure coherent and effective implementation of the right to be forgotten within the broader digital governance architecture. Such coordination would also reduce the risk of regulatory fragmentation and forum shopping by data controllers seeking to exploit gaps between different oversight regimes.

Conclusion

This research has examined the legal framework for personal data protection in Uzbekistan and identified significant deficiencies in current legislation, with particular focus on the absence of a right to be forgotten. The 2019 Law on Personal Data, while representing an important step forward, falls substantially short of international standards in several critical respects: it does not recognize an explicit and enforceable right to erasure; its enforcement framework is inadequate to deter violations by large data controllers; its territorial scope is insufficiently clear with respect to foreign digital platforms; and it relies excessively on a consent-based model that places an unrealistic burden of protection on individual data subjects. These gaps leave Uzbek citizens without effective legal recourse against the harms caused by the permanent availability of outdated, inaccurate, or harmful personal data in the digital

environment, representing both a human rights deficit and a barrier to the country's full integration into the global digital economy.

The comparative analysis of the GDPR, Russian Federal Law No. 264-FZ, the Kazakhstani data protection framework, and Convention has identified a set of legislative best practices and principles that Uzbekistan could adapt in designing its own right to be forgotten. These include: explicit recognition of the right to erasure as a fundamental data subject right with defined triggering conditions and clear procedural mechanisms; a dedicated right to de-indexing applicable to search engine operators; a substantially strengthened enforcement framework with deterrent administrative fines and a private right of action; extraterritorial application to foreign data controllers processing data of Uzbek citizens; and robust exceptions to protect freedom of expression, public interest journalism, and scientific research. The phased implementation of these elements, beginning with targeted search engine delisting and progressing to a more comprehensive erasure framework, offers a practical path forward that balances the urgency of legislative reform against the institutional and technical capacity constraints facing Uzbekistan at its current stage of legal and digital development.

The broader implications of this research extend to Uzbekistan's digital governance agenda and its integration into the global digital economy. A robust right to be forgotten, embedded within a comprehensively reformed personal data protection framework, would enhance public trust in digital services, signal Uzbekistan's commitment to international human rights standards, and support the country's ambitions for digital transformation and international partnership. The proposed reforms should not be viewed in isolation but as part of a comprehensive agenda for modernizing Uzbekistan's digital governance framework, encompassing data portability, algorithmic accountability, and enhanced protection for vulnerable categories of data subjects. Future research should examine empirically the current state of data protection compliance in Uzbekistan, assess public awareness and attitudes toward digital privacy rights, and explore in greater detail the technical and institutional requirements for effective implementation of the proposed reforms. Continued engagement between legal scholars, technologists, policymakers, and civil society will be essential to develop the adaptive, forward-looking legal framework that Uzbekistan's digital future requires and that its citizens deserve.

Bibliography

Abdurakhmanov, A. (2021). Digital governance and personal data protection in Uzbekistan: Current state and reform perspectives. *Journal of Central Asian Law and Society, 8*(2), 45–67.

Ambrose, M. L., & Ausloos, J. (2013). The right to be forgotten across the pond. *Journal of Information Policy, 3*, 1–23. https://doi.org/10.5325/jinfopoli.3.2013.0001

Ausloos, J. (2012). The "right to be forgotten" worth remembering? *Computer Law & Security Review, 28*(2), 143–152. https://doi.org/10.1016/j.clsr.2012.01.006

Bennett, C. J., & Raab, C. D. (2006). *The governance of privacy: Policy instruments in global perspective*. MIT Press.

Koops, B. J. (2011). Forgetting footprints, shunning shadows: A critical analysis of the "right to be forgotten" in big data practice. *SCRIPTed, 8*(3), 229–256. https://doi.org/10.2966/scrip.080311.229

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. https://doi.org/10.1016/j.clsr.2013.03.010

Mayer-Schönberger, V. (2009). *Delete: The virtue of forgetting in the digital age*. Princeton University Press.

McKenna, B., & Bell, J. (2017). Comparative law and legal culture: A methodological overview. *Oxford Journal of Legal Studies, 37*(1), 1–25. https://doi.org/10.1093/ojls/gqw022

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.

Rosen, J. (2012). The right to be forgotten. *Stanford Law Review Online, 64*, 88–92.

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review, 126*(7), 1880–1903.

Yusupov, B. (2020). Data protection law in Central Asia: Challenges and reform imperatives. *Eurasian Law Journal, 12*(4), 112–130.