



DRAFT CYBERSECURITY PROVISION IN THE LAW OF THE REPUBLIC OF UZBEKISTAN “ON INTERNATIONAL COMMERCIAL ARBITRATION”: CONCEPTUAL JUSTIFICATION AND STRUCTURE

Kaibyldaeva Begaim Mukhitovna

Independent Researcher, Tashkent State University of Law

E-mail: begaimkaibyldaeva@gmail.com

<https://doi.org/10.5281/zenodo.20269454>

ARTICLE INFO

Received: 14th May 2026

Accepted: 16th May 2026

Online: 18th May 2026

KEYWORDS

This legislative gap, which was perhaps understandable at the time of the Law's adoption, has become increasingly consequential given the rapid expansion of Uzbekistan's arbitration infrastructure, the country's ambitious digital transformation program under the “Digital Uzbekistan 2030” strategy, and the growing international expectation that arbitration laws should address cybersecurity as a core element of procedural governance

ABSTRACT

The global proliferation of digital technologies has fundamentally restructured the procedural architecture of international commercial arbitration. Electronic document management platforms, cloud-based evidence repositories, encrypted communication channels, and virtual hearings conducted across multiple jurisdictions have become standard features of contemporary arbitral proceedings. These developments have brought undeniable efficiency gains: reduced costs and time associated with physical document production, greater accessibility for geographically dispersed parties, and enhanced flexibility in scheduling procedural steps. Nevertheless, the same digital infrastructure that enables these benefits simultaneously exposes arbitral proceedings to a spectrum of cybersecurity threats, ranging from unauthorized access to confidential case files and interception of legal strategy communications to ransomware attacks targeting arbitral institutions and deliberate manipulation of electronically stored evidence.

Introduction. The global proliferation of digital technologies has fundamentally restructured the procedural architecture of international commercial arbitration. Electronic document management platforms, cloud-based evidence repositories, encrypted communication channels, and virtual hearings conducted across multiple jurisdictions have become standard features of contemporary arbitral proceedings. These developments have brought undeniable efficiency gains: reduced costs and time associated with physical document production, greater accessibility for geographically dispersed parties, and enhanced flexibility in scheduling procedural steps. Nevertheless, the same digital infrastructure that enables these benefits simultaneously exposes arbitral proceedings to a spectrum of cybersecurity threats, ranging from unauthorized access to confidential case files and interception of legal strategy communications to ransomware attacks targeting arbitral institutions and deliberate manipulation of electronically stored evidence.¹

¹IBA Cybersecurity Guidelines for International Arbitration (2022). International Bar Association. Available at: <https://www.ibanet.org>

This legislative gap, which was perhaps understandable at the time of the Law's adoption, has become increasingly consequential given the rapid expansion of Uzbekistan's arbitration infrastructure, the country's ambitious digital transformation program under the "Digital Uzbekistan 2030" strategy, and the growing international expectation that arbitration laws should address cybersecurity as a core element of procedural governance. The present article undertakes a conceptual analysis of the necessity for and proposed structure of a dedicated cybersecurity provision within the Law of the Republic of Uzbekistan "On International Commercial Arbitration," drawing on comparative analysis of leading international frameworks and the regulatory experience of advanced arbitration jurisdictions.²

Cybersecurity in International Commercial Arbitration: Global Standards and Regulatory Frameworks. The emergence of cybersecurity as a distinct governance concern in international commercial arbitration has been driven both by documented incidents and by systemic risk analysis. High-profile data breaches affecting international law firms, arbitral institutions, and parties to high-value disputes have demonstrated that arbitration confidentiality, a cornerstone of the institution, cannot be presumed in the digital environment without the implementation of affirmative protective measures. In response, international arbitration bodies have developed a range of soft-law instruments establishing cybersecurity standards applicable to arbitral proceedings.³

The most comprehensive of these instruments is the International Bar Association Cybersecurity Guidelines for International Arbitration, adopted in 2022. The IBA Guidelines recommend that arbitral tribunals and parties conduct cyber risk assessments at the outset of proceedings, classify sensitive arbitration data according to established security standards, implement proportionate technical and organizational safeguards throughout the proceedings, and agree upon clear protocols for the notification and remediation of cybersecurity incidents. The Guidelines expressly recognize that the appropriate level of security depends upon the nature and value of the dispute, the sensitivity of the information involved, and the technical capacity of the parties and their representatives.⁴

Complementing the IBA Guidelines, the ICCA-ICC-CPR Cybersecurity Protocol for International Arbitration, published jointly in 2020 by the International Council for Commercial Arbitration, the International Chamber of Commerce, and the International Institute for Conflict Prevention and Resolution, provides a procedural framework for cybersecurity governance in arbitral proceedings. The Protocol proposes that arbitral tribunals be empowered to issue cybersecurity procedural orders, establishes baseline security standards for the electronic transmission of sensitive documents, and recommends

²Republic of Uzbekistan. (2006). Law of the Republic of Uzbekistan "On International Commercial Arbitration" (No. ZRU-23 of October 16, 2006). Vedomosti Oliy Majlisa; UNCITRAL. (2006). UNCITRAL Model Law on International Commercial Arbitration (as amended). United Nations. https://uncitral.un.org/en/texts/arbitration/modellaw/commercial_arbitration

³Born, G. B. (2021). International commercial arbitration (3rd ed., pp. 2841-2845). Kluwer Law International; Smeureanu, I. M. (2011). Confidentiality in international commercial arbitration. Kluwer Law International.

⁴IBA Cybersecurity Guidelines for International Arbitration (2022), Guideline 1 (Cybersecurity Risk Assessment) and Guideline 3 (Cybersecurity Measures). International Bar Association.

the designation of a cybersecurity coordinator responsible for managing the digital security of the proceedings.⁵

At the national legislative level, leading arbitration jurisdictions have increasingly integrated cybersecurity considerations into their regulatory frameworks. Singapore's International Arbitration Act operates within a comprehensive data protection regime, and the SIAC Arbitration Rules incorporate provisions enabling tribunals to adopt protective measures in respect of electronically stored information. England and Wales, undertaking a comprehensive review of the Arbitration Act 1996, have considered codifying tribunal powers in respect of cybersecurity within general case management provisions. Hong Kong's HKIAC Administered Arbitration Rules similarly empower tribunals to issue orders concerning the security of electronically stored materials.⁶

Legislative Gap Analysis: Uzbekistan's Law on International Commercial Arbitration. A structural analysis of the Law of the Republic of Uzbekistan "On International Commercial Arbitration" (2021) reveals that the instrument, while faithfully replicating the architecture of the UNCITRAL Model Law, contains no provisions specifically addressing cybersecurity risks arising in the context of digital arbitral proceedings. The provisions governing interim measures (Article 17), the conduct of proceedings (Article 19), and evidence (Article 27) are framed in terms that predate the routine use of electronic communications and cloud-based platforms as the primary medium for arbitration. No mechanism exists within the Law for a tribunal to issue cybersecurity-specific procedural orders, to prescribe data classification standards for sensitive arbitration materials, or to respond to unauthorized disclosure of confidential arbitration data through digital channels.⁷

This legislative gap is not remedied by the general framework of Uzbekistan's information security legislation. The Law "On Informatization" and related Presidential Decrees on cybersecurity establish a general legal regime for the protection of critical information infrastructure and the prevention of cyber incidents affecting public sector and commercially significant information systems. However, these instruments do not specifically address the international commercial arbitration context, where the confidentiality of proceedings, the cross-jurisdictional nature of parties' operations, and the institutional independence of arbitral tribunals create specialized regulatory challenges that fall outside the scope of general public cybersecurity governance.⁸

Similarly, the Law of the Republic of Uzbekistan "On Personal Data" (No. ZRU-547 of July 2, 2019) imposes obligations on data operators and processors to implement appropriate technical and organizational security measures for personal data. While some arbitration

⁵International Council for Commercial Arbitration, International Chamber of Commerce, & International Institute for Conflict Prevention and Resolution. (2020). ICCA-ICC-CPR Cybersecurity Protocol for International Arbitration. ICCA Publications. Available at: <https://www.arbitration-icca.org/publications/cybersecurity-protocol>

⁶Singapore International Arbitration Centre. (2025). SIAC Arbitration Rules 2025 (Rule 19 on Directions for Conduct of Proceedings). SIAC; HKIAC Administered Arbitration Rules 2018, Article 22.3; Lew, J. D. M., Mistelis, L. A., & Kroll, S. M. (2003). Comparative international commercial arbitration (pp. 543-548). Kluwer Law International.

⁷Republic of Uzbekistan. (2006). Law of the Republic of Uzbekistan "On International Commercial Arbitration," Articles 17, 19, 27 (No. ZRU-23 of October 16, 2006). Vedomosti Oliy Majlisa; UNCITRAL. (2016). Notes on organizing arbitral proceedings. United Nations.

⁸Republic of Uzbekistan. (2003). Law of the Republic of Uzbekistan "On Informatization" (as amended). Vedomosti Oliy Majlisa; President of the Republic of Uzbekistan. (2018). Decree "On measures to further improve the cybersecurity system of the Republic of Uzbekistan." Official Gazette of the Republic of Uzbekistan.

materials will constitute personal data within the meaning of this Law, arbitral proceedings frequently involve commercially sensitive information, strategic business data, financial projections, and proprietary technical information that falls outside the scope of personal data protection but requires equally rigorous security governance. The absence of a specific cybersecurity provision in the arbitration law therefore leaves a significant regulatory space unaddressed.⁹

The significance of this gap is heightened by the increasing operational activity of the Tashkent International Arbitration Centre, established in 2018 and progressively developing its caseload in both domestic and international commercial disputes. As TIAC seeks to attract higher-value international proceedings, the absence of clear cybersecurity standards in the governing law of the arbitration seat represents a potential competitive disadvantage relative to jurisdictions whose arbitration frameworks provide greater regulatory certainty in this respect.¹⁰

Conceptual Justification for a Dedicated Cybersecurity Provision. The case for incorporating a specific cybersecurity provision into the Law on International Commercial Arbitration rests on three doctrinal foundations well-established in international arbitration scholarship: the principle of *lex specialis* regulatory precision, the principle of institutional equivalence with leading arbitration seats, and the principle of regulatory complementarity with general data protection legislation.

Under the *lex specialis* principle, the distinctive features of international commercial arbitration party autonomy, confidentiality, cross-border proceedings, institutional independence require specialized regulatory treatment rather than reliance on general data protection or information security legislation. General cybersecurity laws are calibrated to public sector and commercial enterprise contexts; they are not designed to address the specific dynamics of confidential international dispute resolution, where the stakes of a data breach extend beyond financial harm to encompass the potential compromise of legal strategy, the undermining of arbitral impartiality, and the invalidation of proceedings. A *lex specialis* provision within the arbitration law provides the targeted legal certainty that general legislation cannot supply.¹¹

The principle of institutional equivalence recognizes that Uzbekistan's arbitration law must meet standards comparable to those prevailing in competing arbitration seats. The adoption by the IBA and ICCA of comprehensive cybersecurity standards, and their incorporation into the rules of leading arbitral institutions including SIAC, HKIAC, and the ICC International Court of Arbitration, has established a *de facto* international benchmark against which the adequacy of Uzbekistan's legal framework will be assessed by sophisticated commercial parties and their legal counsel.¹²

⁹Republic of Uzbekistan. (2019). Law of the Republic of Uzbekistan "On Personal Data" (No. ZRU-547 of July 2, 2019), Articles 9-11. Vedomosti Oliy Majlisa.

¹⁰Tashkent International Arbitration Centre. (2022). Annual Report 2022. Available at: <https://tiac.uz>; Born, G. B. (2021). International commercial arbitration (3rd ed., pp. 236-240). Kluwer Law International.

¹¹Born, G. B. (2021). International commercial arbitration (3rd ed., pp. 2189-2195). Kluwer Law International; Schreuer, C., Malintoppi, L., Reinisch, A., & Sinclair, A. (2009). The ICSID Convention: A commentary (2nd ed., pp. 391-396). Cambridge University Press.

¹²IBA Cybersecurity Guidelines for International Arbitration (2022), Preamble; ICCA-ICC-CPR Cybersecurity Protocol for International Arbitration (2020), Protocol 1 (Baseline Standards). ICCA Publications.

The principle of regulatory complementarity acknowledges that a cybersecurity provision in the arbitration law would not merely duplicate existing data protection obligations but would perform a constitutive function: establishing the standard of care owed by tribunals, institutions, and parties in relation to the digital assets of arbitral proceedings; creating a legal basis for cybersecurity-specific interim measures and procedural orders; and providing a framework for the allocation of liability and procedural consequences in the event of a security breach. These are functions that neither the general information security regulations nor the Law on Personal Data (2019) is designed to perform in the international arbitration context.

Proposed Structure of the Draft Cybersecurity Provision. Drawing on the IBA Cybersecurity Guidelines (2022), the ICCA-ICC-CPR Protocol (2020), and comparative legislative practice in leading arbitration jurisdictions, the following structure for a draft cybersecurity provision in the Law of the Republic of Uzbekistan "On International Commercial Arbitration" is proposed. The provision would most appropriately be inserted as Article 17-1, following the existing interim measures provision, or incorporated as a discrete Chapter IV-A within the Law.

The first operative element of the draft provision would be a definitional clause, establishing the meaning of the key terms "cybersecurity incident," "sensitive arbitration data," "digital arbitration infrastructure," and "cybersecurity order." The definitions should be aligned with the terminology employed in the relevant Uzbek legislation while reflecting the specific characteristics of international commercial arbitration as defined in Article 1 of the existing Law.¹³

The second element would be a general duty of cybersecurity care, imposing upon the arbitral tribunal, any administering arbitral institution, and the parties a proportionate obligation to implement and maintain technical and organizational security measures adequate to protect sensitive arbitration data from unauthorized access, disclosure, modification, or destruction throughout the arbitral proceedings. The standard of proportionality would be assessed by reference to the nature and value of the dispute, the sensitivity of the information involved, and the technical and financial resources of the parties, consistent with the risk-based approach of the IBA Cybersecurity Guidelines.

The third element would be a data classification and handling clause, requiring the parties and the tribunal to agree, at an early stage of proceedings, upon a classification scheme for arbitration materials in terms of their sensitivity and the corresponding security requirements for storage, transmission, and access. This clause would empower the tribunal to issue a cybersecurity procedural order establishing minimum security standards applicable to the parties, their legal representatives, and expert witnesses.¹⁴

The fourth element would be an incident response clause, establishing mandatory notification obligations upon any party, representative, or arbitral institution that discovers a cybersecurity incident materially affecting the confidentiality or integrity of arbitration

¹³UNCITRAL. (2016). Notes on organizing arbitral proceedings, Notes 35-41 (Electronic communications and online hearings). United Nations; Republic of Uzbekistan. (2019). Law "On Personal Data" (No. ZRU-547), Article 3 (Definitions).

¹⁴ICCA-ICC-CPR Cybersecurity Protocol for International Arbitration (2020), Schedules A and B (Minimum Baseline Cybersecurity Standards). ICCA Publications.

materials. The clause would specify the timeframe and form of notification, the party or authority to be notified, and the immediate remedial measures to be taken. Where a cybersecurity incident involves the unauthorized disclosure of personal data, the clause would require parallel compliance with the notification obligations of the Law on Personal Data (2019).

The fifth element would be a sanctions and remedies clause, addressing the procedural and substantive consequences of failures to comply with cybersecurity obligations. The tribunal would be empowered to draw adverse inferences from evidence obtained through security failures attributable to a party, to order the exclusion of evidence whose integrity has been compromised, and to award security-related costs against a party whose non-compliance caused additional procedural expense. This element provides the enforcement mechanism that distinguishes the proposed statutory provision from the non-binding soft-law instruments currently available at the international level.¹⁵

Recommendations for Legislative Implementation. The adoption of the proposed cybersecurity provision requires a coordinated approach involving governmental, institutional, and professional actors. In the legislative sphere, the Ministry of Justice of the Republic of Uzbekistan, in consultation with the Tashkent International Arbitration Centre and independent experts in international arbitration law and information security, should develop a draft amendment to the Law on International Commercial Arbitration incorporating the provision described above. The drafting process should include formal public consultation to ensure alignment with current industry practice and the soft-law frameworks developed by the IBA and ICCA.

In the institutional sphere, the Tashkent International Arbitration Centre should develop a dedicated Cybersecurity Annex to its Arbitration Rules, operationalizing the obligations established in the legislative provision through specific procedural mechanisms tailored to the characteristics of TIAC proceedings. This Annex should include a model cybersecurity procedural order for tribunal use and a template cybersecurity agreement for adoption by parties at the commencement of proceedings.

In the area of international engagement, Uzbekistan should consider acceding to the Budapest Convention on Cybercrime (Council of Europe, 2001), which is open to non-member states, as a complementary measure enhancing the country's capacity to address cross-border cybersecurity incidents affecting arbitral and judicial proceedings. Such accession would signal the country's commitment to international cybersecurity governance standards and would strengthen the legal framework for cooperation with foreign authorities in cases involving cyber incidents with a cross-border dimension.

Conclusion. The absence of cybersecurity provisions in the Law of the Republic of Uzbekistan "On International Commercial Arbitration" represents a significant and increasingly consequential gap in the national arbitration legal framework. The progressive digitalization of international arbitration, the emergence of robust soft-law standards through the IBA Cybersecurity Guidelines (2022) and the ICCA-ICC-CPR Protocol (2020), and the strategic imperative of positioning Uzbekistan as a credible arbitration seat in the Central

¹⁵Born, G. B. (2021). International commercial arbitration (3rd ed., pp. 2851-2860). Kluwer Law International; IBA Cybersecurity Guidelines for International Arbitration (2022), Guideline 5 (Incident Response and Notification).

Asian region collectively mandate the adoption of a dedicated legislative provision addressing cybersecurity risks in arbitral proceedings.

The proposed provision, structured around the five operative elements of definitional clarity, a general duty of cybersecurity care, data classification, incident response, and a sanctions regime, provides a legally sound and operationally practical framework for addressing cybersecurity risks in Uzbekistan's international commercial arbitration proceedings. Its adoption would signal Uzbekistan's commitment to a legal infrastructure commensurate with international standards and would enhance the attractiveness of the country as a venue for the resolution of high-value cross-border disputes.

Further research in this area should address the comparative implementation experience of cybersecurity provisions in arbitration laws across Central Asian jurisdictions, the interaction between the proposed provision and Uzbekistan's data protection framework, and the specific challenges posed by the cybersecurity of online dispute resolution mechanisms in investor-state arbitration proceedings

References:

1. Born, G. B. (2021). International commercial arbitration (3rd ed.). Kluwer Law International.
2. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention), CETS No. 185. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
3. International Bar Association. (2022). IBA cybersecurity guidelines for international arbitration. International Bar Association. <https://www.ibanet.org>
4. International Council for Commercial Arbitration, International Chamber of Commerce, & International Institute for Conflict Prevention and Resolution. (2020). ICCA-ICC-CPR cybersecurity protocol for international arbitration. ICCA Publications. <https://www.arbitration-icca.org/publications/cybersecurity-protocol>
5. Lew, J. D. M., Mistelis, L. A., & Kroll, S. M. (2003). Comparative international commercial arbitration. Kluwer Law International.
6. Republic of Uzbekistan. (2003). Law of the Republic of Uzbekistan "On Informatization" (as amended). Vedomosti Oliy Majlisa.
7. Republic of Uzbekistan. (2021). Law of the Republic of Uzbekistan "On International Commercial Arbitration" Vedomosti Oliy Majlisa.
8. Republic of Uzbekistan. (2019). Law of the Republic of Uzbekistan "On Personal Data" (No. ZRU-547 of July 2, 2019). Vedomosti Oliy Majlisa.
9. Schreuer, C., Malintoppi, L., Reinisch, A., & Sinclair, A. (2009). The ICSID Convention: A commentary (2nd ed.). Cambridge University Press.
10. Singapore International Arbitration Centre. (2025). SIAC Arbitration Rules 2025. SIAC. <https://siac.org.sg>
11. Smeureanu, I. M. (2011). Confidentiality in international commercial arbitration. Kluwer Law International.
12. Tashkent International Arbitration Centre. (2022). Annual report 2022. TIAC. <https://tiac.uz>
13. UNCITRAL. (2006). UNCITRAL Model Law on International Commercial Arbitration (as amended). United Nations. https://uncitral.un.org/en/texts/arbitration/modellaw/commercial_arbitration
14. UNCITRAL. (2016). Notes on organizing arbitral proceedings. United Nations.

15.UNCTAD. (2023). World investment report 2023: Investing in sustainable energy for all. United Nations. <https://unctad.org/wir2023>

