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

Confidentiality and Data Protection in International Commercial Arbitration: Civil Law Aspects of Digital Risk Management

Kaibildaeva Begaim Mukhitovna
Tashkent State University of Law

Abstract

International commercial arbitration increasingly operates within digital environments, generating complex questions about confidentiality obligations and personal data protection under civil law. This research examines how the duty of confidentiality in arbitral proceedings intersects with modern data protection regimes, particularly in contexts shaped by cross-border digital data flows, cloud-based case management, and artificial intelligence-assisted dispute resolution. Using a qualitative doctrinal methodology, the study analyses international arbitration rules, national civil law frameworks, and data protection legislation including the GDPR and analogous instruments. The findings reveal that existing confidentiality norms are inadequate to address digital risks such as unauthorized data access, cyber intrusions, and transcoder data transfers. The study concludes that harmonized, technology-sensitive legal standards are urgently needed to ensure that arbitral confidentiality is meaningfully preserved in the digital age, and recommends proactive reforms to institutional rules, national statutes, and practitioner guidelines.

Keywords: Confidentiality, International Commercial Arbitration, Data Protection, Digital Risk Management, Civil Law, GDPR, Cybersecurity, Cross-Border Data Transfer

APA Citation:

Kaibildaeva, B. (2026). Confidentiality and Data Protection in International Commercial Arbitration: Civil Law Aspects of Digital Risk Management. *Uzbek Journal of Law and Digital Policy, 4*(2), 38–56. https://doi.org/10.59022/ujldp.538

I. Introduction

Imagine a highly sensitive international commercial dispute involving trade secrets, financial projections, and personal data of corporate executives being administered entirely through a cloud-based arbitration platform, with submissions shared via encrypted email, hearings conducted by video conference, and the final award stored on servers located in multiple jurisdictions. This scenario is no longer hypothetical. The rapid digitization of international commercial arbitration has transformed the procedural landscape, but the legal frameworks governing confidentiality and data protection have not kept pace with that transformation. The traditional promise of privacy and confidentiality that makes arbitration attractive to commercial parties is increasingly undermined by the technical realities of digital data management. Regulators, arbitrators, and practitioners must now confront a fundamental question: what does it mean to keep arbitral proceedings confidential when data flows across borders, resides in foreign servers, and may be subject to state surveillance or cybercriminal exploitation?

International commercial arbitration has long been celebrated as a private form of dispute resolution, offering parties control over the process, confidentiality of proceedings, and enforceability of awards through the New York Convention (Born, 2021). These attributes distinguish arbitration from public litigation and account for its widespread adoption in transnational commerce. Confidentiality, though not universally recognized as an implied obligation under all national legal systems, is embedded in the rules of most leading arbitral institutions, including the International Chamber of Commerce (ICC), the London Court of International Arbitration (LCIA), and the Singapore International Arbitration Centre (SIAC). However, the digital transformation of dispute resolution encompassing electronic filing systems, virtual hearings, artificial intelligence tools, and remote document review platforms has created new vectors for confidentiality breaches. Data breaches, inadvertent disclosures, and unlawful processing of personal data contained in case files are among the most pressing risks now facing arbitral proceedings.

The intersection of arbitral confidentiality with data protection law presents particular complexity for civil law systems. Civil law jurisdictions prevalent across Continental Europe, Latin America, East Asia, and Central Asia approach the relationship between private agreements and statutory obligations differently from their common law counterparts (Cordero-Moss, 2019). The general principle in civil law systems is that statutory rules, including those governing personal data protection, are mandatory and override any contractual or procedural arrangements. This means that arbitration agreements and institutional rules purporting to create absolute confidentiality may be displaced or qualified by data protection obligations imposed by legislation such as the European Union General Data Protection Regulation (GDPR), Uzbekistan's Law on Personal Data of 2019, and similar instruments. Understanding how these obligations co-exist or conflict with arbitral confidentiality

is a matter of growing practical importance, yet the academic and regulatory literature on this intersection remains underdeveloped.

The digitalization of arbitral proceedings has generated several concrete risks that implicate both confidentiality and data protection. First, cyber intrusions targeting arbitration institutions and law firms have demonstrated that even sophisticated digital infrastructures can be compromised, resulting in the exposure of sensitive commercial and personal information. Second, the use of cloud computing and third-party service providers in case management raises questions about data controller and processor responsibilities under privacy regulations. Third, virtual hearings transmitted over commercial video conferencing platforms may involve the processing of biometric and personal data in ways that are not contemplated by existing arbitration rules. Fourth, artificial intelligence tools used for document review or predictive analysis may process personal data in ways that require specific legal justification and raise concerns about automated decision-making. Each of these risks challenges the assumption that arbitral proceedings can be adequately shielded from the external legal environment through institutional rules and party agreements alone.

Despite the urgency of these issues, existing scholarship tends to treat arbitral confidentiality and data protection as parallel but separate legal concerns. Technical literature on cybersecurity in dispute resolution focuses on system architecture and best practices rather than legal obligations. Legal scholarship on arbitral confidentiality examines the doctrinal foundations and comparative frameworks of the duty without systematically addressing its digital dimensions (Bühring-Uhle et al., 2020). Data protection scholarship, meanwhile, rarely engages with the specific institutional context of arbitration. Scholarship addressing civil law approaches to digital risk management in arbitration is particularly sparse, despite the fact that civil law systems host many of the world's most important arbitral seats and generate a large proportion of international commercial disputes. This research gap is the primary motivation for the present study, which seeks to analyses the civil law dimensions of confidentiality and data protection in international commercial arbitration from the perspective of digital risk management.

The objectives of this research are threefold. First, to examine how confidentiality obligations in international commercial arbitration are defined and enforced across major civil law jurisdictions and institutional frameworks. Second, to analyses how data protection legislation with particular focus on the GDPR and its analogues in civil law countries interacts with arbitral confidentiality duties in the context of digital proceedings. Third, to identify the key digital risks that threaten arbitral confidentiality and personal data protection, and to propose legal and institutional reforms capable of addressing those risks. The central research question guiding the study is: how can civil law frameworks for confidentiality and data protection be adapted to adequately govern digital risk management in international commercial arbitration? This question connects doctrinal analysis with institutional

design, and its answer has practical consequences for parties, arbitrators, institutions, and legislators across the global arbitration community.

The significance of this study is multifold. As digital arbitration becomes the norm rather than the exception a trend dramatically accelerated by the COVID-19 pandemic the legal uncertainty surrounding confidentiality and data protection creates tangible risks for commercial parties and weakens confidence in arbitration as a dispute resolution mechanism. The study contributes to filling the gap between technology and law in the arbitration context, offering a doctrinal analysis grounded in comparative civil law methodology. It is also practically relevant, providing guidance for institutional rule revision, legislative drafting, and practitioner conduct. Finally, the study contributes to the broader literature on digital governance and private international law, situating the arbitration confidentiality problem within the wider challenge of managing cross-border data flows in a multipolar legal world.

II. Methodology

This study adopts a qualitative research design grounded in doctrinal legal analysis and comparative methodology. The doctrinal approach is appropriate because the research seeks to understand, interpret, and critique existing legal rules, principles, and standards rather than to measure empirical phenomena. Comparative methodology is employed to examine how different civil law jurisdictions and international instruments approach the dual obligations of arbitral confidentiality and data protection, identifying convergences, divergences, and reform opportunities. The study does not generate primary empirical data but engages analytically with a carefully selected body of legal texts, institutional documents, and scholarly literature to construct a coherent picture of the current legal framework and its deficiencies.

The research population for the study consists of the body of legal instruments, institutional rules, and authoritative commentary governing confidentiality and data protection in international commercial arbitration, with emphasis on civil law systems. The sample is purposively selected to ensure coverage of the most significant and influential sources. Primary legal sources include the ICC Rules of Arbitration 2021, the LCIA Arbitration Rules 2020, the SIAC Arbitration Rules 2016, the UNCITRAL Arbitration Rules 2013, the UNCITRAL Model Law on International Commercial Arbitration, and the New York Convention 1958. National legislative sources include the GDPR (EU Regulation 2016/679), the French Code of Civil Procedure, the Swiss Private International Law Act, German civil procedure statutes, Uzbekistan's Law on Personal Data 2019, and analogous instruments from other civil law jurisdictions in Asia and Latin America.

Data collection proceeds through systematic review of the selected sources using publicly accessible legal databases including EUR-Lex, UNCITRAL's online resources, the websites of leading arbitral institutions, and peer-reviewed legal databases such as Westlaw International, HeinOnline, and Google Scholar. The

inclusion criteria require that all sources be either currently in force, constitute authoritative interpretive guidance, or represent peer-reviewed scholarship published within the past decade, ensuring currency and relevance. All sources are assessed for authenticity by reference to official publications, institutional authorship, and citation frequency in the scholarly literature. No human participants are involved in the research, eliminating the need for institutional ethics review, though the study is conducted with full regard for academic integrity and intellectual property obligations.

The analytical framework combines three complementary methodological techniques. First, doctrinal analysis is used to identify the normative content of confidentiality obligations in arbitration law and data protection law, establishing the legal standards against which practice can be evaluated. Second, comparative analysis is used to examine how these obligations are framed across multiple civil law systems, highlighting areas of harmonization and fragmentation. Third, a digital risk management lens is applied to assess the adequacy of existing legal frameworks in addressing the specific threats associated with digital arbitration, including cyber intrusions, unlawful data processing, and cross-border data transfers. This combined framework enables the study to move from descriptive analysis to normative critique and prescriptive recommendation.

Limitations of the methodology include the inherent selectivity of doctrinal analysis, which necessarily emphasizes official legal texts over informal norms and practical realities. The comparative scope, while broad, cannot encompass every civil law jurisdiction, and the study acknowledges that significant variation exists within the civil law tradition. Reliance on publicly available sources may also mean that some institutional practices and unpublished arbitral awards which are they confidential are not fully reflected in the analysis. Notwithstanding these limitations, the study's findings are grounded in authoritative sources and are cross-referenced across multiple jurisdictions and institutional frameworks to ensure robustness and reliability. The study's delimitations are set by focusing on commercial arbitration rather than investment arbitration, and on civil law systems rather than common law, reflecting the specific research objectives and avoiding excessive breadth.

III. Results

The document analysis conducted for this study reveals a complex and fragmented legal landscape governing confidentiality and data protection in digital commercial arbitration. The central research question how civil law frameworks can be adapted to address digital risk management in international arbitration yields findings that are simultaneously encouraging and sobering. On the encouraging side, both arbitral institutions and data protection regulators have taken preliminary steps toward addressing digital risks; on the sobering side, these efforts are piecemeal, inconsistent, and largely insufficient to address the full range of threats posed by digital proceedings. The analysis identifies four principal finding clusters: the nature

and limits of existing confidentiality obligations; the applicability and scope of data protection law in arbitral contexts; the principal digital risks and their legal implications; and the emerging regulatory and institutional responses.

The first finding concerns the normative foundations of arbitral confidentiality in civil law systems. Most leading civil law jurisdictions do not recognize an implied duty of confidentiality in arbitration as a matter of national law; instead, confidentiality obligations derive from institutional rules, party agreements, or specific statutory provisions. The French Code of Civil Procedure, for example, imposes a general professional secrecy obligation on arbitrators but leaves confidentiality of proceedings largely to party agreement (Rosenthal, 2020). The Swiss Private International Law Act is similarly silent on confidentiality, relying on institutional rules to fill the gap. German law follows a comparable approach. By contrast, the LCIA Rules 2020 contain some of the most detailed confidentiality provisions in institutional arbitration, imposing obligations on parties, arbitrators, and the institution itself. The ICC, historically more restrained, strengthened its approach in the 2021 Rules. SIAC and other Asian institutions have also progressively elaborated their confidentiality provisions. The result is a patchwork of obligations whose scope and enforceability depend heavily on the governing rules, the seat of arbitration, and the applicable law.

The second finding concerns the applicability of data protection law to arbitral proceedings. The GDPR's broad territorial scope applying to processing of personal data by controllers established in the EU and to the processing of data of EU data subjects regardless of where processing occurs means that it is frequently applicable to international commercial arbitration even where proceedings are seated outside the EU. The analysis reveals that arbitral institutions, law firms, parties, and arbitrators each potentially qualify as data controllers or processors under the GDPR's definitions, though the precise allocation of responsibilities has not been systematically addressed in either regulatory guidance or institutional practice (Lachmann, 2022). Data subjects whose personal information appears in arbitral submissions, witness statements, or financial records have rights including rights of access, erasure, and objection to automated processing that may conflict with the confidentiality and integrity of arbitral proceedings. The tension between data subject rights and arbitral confidentiality has no clear resolution under existing law.

The third finding cluster concerns the principal digital risks identified in the analysis. Cyber intrusions targeting arbitral institutions and their service providers have occurred with increasing frequency; notable incidents at major law firms and international organizations have demonstrated the feasibility of large-scale data breaches affecting arbitral files. Cloud computing introduces risks of unauthorized access, data localization conflicts with national law requirements, and potential government access to data hosted by cloud providers subject to foreign national security legislation such as the US CLOUD Act. Virtual hearing platforms process

audio, video, and potentially biometric data of participants, raising data minimization and purpose limitation concerns under the GDPR and analogous instruments. AI-assisted document review tools, increasingly used in large arbitrations, may process personal data at scale without adequate legal basis. Each of these risks creates potential for liability both civil liability for breach of confidentiality and regulatory liability for data protection violations that existing arbitration rules and national civil law frameworks have not adequately addressed.

The fourth finding concerns emerging regulatory and institutional responses. The ICC Data Protection Guidance Note of 2022 represents perhaps the most substantive institutional attempt to address the interface between GDPR obligations and arbitral practice, offering guidance on legal bases for processing, data retention, and the handling of data subject requests. The LCIA has updated its privacy notice and introduced case management practices designed to reduce unnecessary personal data processing. UNCITRAL has noted the need for further work on cybersecurity in arbitration but has not yet produced binding or authoritative guidance. At the national level, the EU's proposed Artificial Intelligence Act introduces requirements that may apply to AI tools used in arbitration. Uzbekistan, as part of its broader digital governance reform program, has enacted data protection legislation that applies to personal data processing by arbitral institutions operating within its territory, though implementation guidance for arbitral contexts is lacking. These developments are positive but scattered, lacking the coherence and authority needed to establish a reliable framework for digital risk management in international arbitration.

IV. Discussion

A. Confidentiality and Privacy as Distinct but Overlapping Values

Any meaningful analysis of confidentiality and data protection in international commercial arbitration must begin by distinguishing the two concepts while recognizing their significant overlap in digital contexts. Confidentiality in arbitration is a procedural and contractual norm that restricts disclosure of information about arbitral proceedings to third parties, protecting the privacy of the dispute resolution process itself (Moses, 2017). It is grounded in the parties' expectation of privacy from the public sphere, the sensitivity of commercial information, and the institutional logic of private adjudication. Data protection, by contrast, is a regulatory regime governing the processing of personal data, protecting individuals from having their personal information processed in ways that threaten their autonomy, dignity, or fundamental rights. It is grounded in human rights norms and operates as mandatory law, applicable regardless of contractual arrangements. While confidentiality is primarily concerned with secrecy as between arbitral participants and the outside world, data protection is concerned with the lawfulness, fairness, and transparency of data processing as between data controllers and individual data subjects.

In the digital arbitration environment, these two frameworks interact in complex

and sometimes contradictory ways. Confidentiality obligations may actually reinforce data protection in certain respects for example, by preventing the disclosure of personal information in arbitral submissions to third parties. Conversely, data subject rights to access their personal data held by arbitral institutions may potentially expose confidential arbitral materials to parties who are themselves data subjects but whose access rights have not been specifically limited by applicable law (Kaufmann-Kohler & Rigozzi, 2021). The right to erasure could, if applied to arbitral records, undermine the integrity of the award and the arbitral record. Automated processing of personal data through AI tools raises particular concerns because the GDPR's prohibition on solely automated decision-making with legal or similarly significant effects may apply to certain uses of predictive AI in arbitration. Understanding the conceptual relationship between these frameworks is therefore essential to developing coherent legal responses to digital risk in arbitration.

Civil law doctrine provides important resources for navigating this interface. In civil law systems, the hierarchy of norms constitutional rights, mandatory legislation, public policy establishes clear priority rules for conflicts between statutory obligations and private arrangements. Data protection legislation, as mandatory law, takes priority over contractual confidentiality clauses and institutional arbitration rules where they conflict. This principle of statutory supremacy means that parties and institutions cannot validly contract out of data protection obligations through arbitration agreements, confidentiality undertakings, or institutional rules, regardless of how those rules are framed. Nor can they invoke arbitral confidentiality as a legal basis for refusing to comply with data subject access requests or regulatory investigations. At the same time, civil law doctrine of private autonomy preserves substantial space for parties to structure their arbitration agreements and confidentiality obligations within the limits set by mandatory law. The civil law framework thus demands that arbitral confidentiality and data protection be reconciled through careful legal drafting, institutional adaptation, and where necessary legislative reform.

B. Civil Law Dimensions of Arbitral Confidentiality

The treatment of arbitral confidentiality across civil law jurisdictions reveals significant variation alongside shared structural features. In France, the confidentiality of arbitral proceedings is strongly associated with the notion of professional secrecy, which is a general obligation applicable to legal professionals and judicial officers including arbitrators. Article 1464 of the French Code of Civil Procedure provides that deliberations of the arbitral tribunal are confidential, but this provision does not extend to the proceedings as a whole in the absence of party agreement or applicable institutional rules. French courts have recognized an implied duty of confidentiality in certain circumstances, particularly where the nature of the information processed in the arbitration clearly warrants protection, but the scope and enforceability of this implied duty in the digital context remain uncertain (Mourre, 2021).

Swiss law, which governs one of the world's most important arbitral seats, treats

confidentiality primarily as a matter of party agreement and institutional rules rather than statutory obligation. The Swiss Rules of International Arbitration 2021, administered by the Swiss Arbitration Centre, contain detailed confidentiality provisions applying to parties, the institution, and arbitrators. However, the Swiss Private International Law Act itself does not impose a general confidentiality obligation on arbitral proceedings, leaving the matter to party choice and institutional governance. This approach reflects the Swiss emphasis on party autonomy in international commercial arbitration, but it also means that confidentiality protections are only as strong as the contractual or institutional framework chosen by the parties. In a digital environment where data processing obligations may be imposed by regulation regardless of party choice, the adequacy of a purely contractual approach to confidentiality becomes questionable.

German law presents yet another variation. The German Code of Civil Procedure (Zivilprozessordnung, ZPO) governs domestic arbitration and applies subsidiary to international arbitrations seated in Germany, supplemented by the German Arbitration Institute (DIS) Rules 2018. The DIS Rules contain an express confidentiality provision requiring parties, arbitrators, and institutions to maintain confidentiality of all information relating to the arbitration. German courts have generally upheld contractual confidentiality obligations in arbitration, treating them as enforceable under general principles of contract law. However, German data protection law shaped by both the GDPR and national implementation legislation imposes obligations that can override contractual arrangements where they conflict with statutory rights of data subjects. The Federal Constitutional Court's strong tradition of protecting fundamental rights, including informational self-determination, creates a constitutional dimension to personal data protection that may further qualify arbitral confidentiality in cases involving personal data of third-party data subjects such as employees or customers whose information appears in arbitral submissions.

In Central Asian civil law systems, including Uzbekistan, the legal framework for arbitral confidentiality is still developing. Uzbekistan's Law on International Commercial Arbitration 2006 and the Tashkent International Arbitration Centre (TIAC) Rules contain confidentiality provisions modelled on UNCITRAL norms, reflecting the country's broader engagement with international commercial law harmonization. The Law on Personal Data of 2019 establishes a comprehensive data protection regime applicable to operators processing personal data of Uzbek nationals, which would include arbitral institutions operating in Uzbekistan and parties processing personal data in the course of arbitral proceedings. The cross-border dimension of data protection compliance is particularly relevant given Uzbekistan's position as an emerging arbitral seat for disputes involving parties from Central Asia, China, and European countries. The regulatory framework is in place but implementation guidance for arbitral contexts is currently absent, creating legal uncertainty for practitioners and institutions.

C. Data Protection Law and Its Application to Arbitral Proceedings

The GDPR, as the world's most comprehensive and widely extraterritorial data protection instrument, provides the most relevant regulatory framework for analyzing the application of data protection law to international commercial arbitration. The GDPR's application to arbitration raises threshold questions about the identification of data controllers and processors within the arbitral process, the legal bases for processing personal data in arbitral proceedings, the exercise of data subject rights in the arbitral context, and the requirements for cross-border data transfers. Each of these questions presents distinctive challenges that have not yet been systematically resolved in regulatory guidance or judicial decisions, creating significant legal uncertainty for arbitral practitioners and institutions.

The question of who is a data controller in an arbitration is particularly complex. The GDPR defines a controller as a natural or legal person who determines the purposes and means of processing personal data. In an arbitration involving multiple parties, arbitrators, and institutions, processing decisions are distributed across these actors. The arbitral institution determines the purposes of processing personal data for case administration and record-keeping. Law firms acting as counsel process personal data for the purposes of representing their clients. Parties themselves process personal data in the course of gathering evidence and preparing submissions. Individual arbitrators process personal data in the course of their decision-making. Technological service providers cloud platforms, video conferencing services, e-discovery tools process personal data as processors under the instructions of controllers. This complex distribution of processing activities requires careful analysis of each actor's role and responsibilities under applicable data protection law, but existing institutional rules and national legislation have not yet provided clear guidance on these allocations.

The legal bases for processing personal data in arbitral proceedings are similarly complex. Under Article 6 of the GDPR, processing requires one of six specified legal bases, including consent, contractual necessity, legal obligation, vital interests, public interest, or legitimate interests. The arbitration agreement between parties provides a contractual basis for processing their own personal data, but may not cover the processing of personal data of third parties witnesses, employees, customers whose data appears in arbitral submissions. Processing based on legitimate interests requires a balancing test between the controller's interests and the data subject's fundamental rights. The extent to which this test can be satisfied in the arbitration context depends on factors that have not been authoritatively determined, including the nature of the data processed, the sensitivity of the arbitral proceedings, and the expectations of third-party data subjects.

Data subject rights present particular challenges for arbitral proceedings. The right of access, under Article 15 of the GDPR, entitles data subjects to receive a copy of personal data held about them, together with information about the processing. If a

data subject whose personal data appears in arbitral documents exercises this right against an arbitral institution or party, the institution or party may be required to disclose confidential arbitral materials. While Article 15(4) allows withholding of information where this would adversely affect the rights and freedoms of others including confidentiality rights of arbitral parties the application of this exception is not straightforward and may require judicial determination. The right to erasure under Article 17 similarly conflicts with the need to maintain an accurate arbitral record. Institutions and parties need clear guidance on how to exercise data subject rights while preserving the integrity of arbitral proceedings, but such guidance is currently lacking in most jurisdictions.

D. Digital Risk Management: Key Threats and Legal Responses

Digital risk management in international commercial arbitration must be understood as a multi-layered challenge involving technical, institutional, contractual, and regulatory dimensions. The principal digital risks identified in this study are cyber intrusions, cloud computing vulnerabilities, virtual hearing security risks, and AI-related data processing risks. Each of these risks creates distinct legal obligations and practical challenges, and each requires a tailored response that integrates technical safeguards with legal and institutional measures. The following analysis addresses each risk category in turn, identifying the applicable legal obligations and the adequacy of current responses.

Cyber intrusions including hacking, ransomware attacks, and data theft represent perhaps the most direct and serious threat to arbitral confidentiality and data protection. Law firms and arbitral institutions have been targeted by sophisticated cyber actors including state-sponsored groups, as evidenced by high-profile incidents involving major international law firms in recent years. These attacks can result in the disclosure of confidential arbitral materials, personal data of parties and witnesses, privileged legal advice, and commercially sensitive information. Under the GDPR, a personal data breach must be notified to the supervisory authority within 72 hours of the controller becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Individuals affected by high-risk breaches must also be notified. These obligations apply to arbitral institutions and law firms processing personal data in the context of arbitration, creating urgent obligations that have not been specifically addressed in institutional rules or arbitral practice guides.

Cloud computing presents a distinct set of risks related to data sovereignty, cross-border transfers, and third-party access. Arbitral institutions and law firms increasingly rely on cloud service providers for document storage, case management, and communication. Data hosted in cloud infrastructure may be subject to access by authorities of the country where the cloud provider is established or where data centers are located, regardless of where the arbitral parties are based or where the arbitration is seated. The US CLOUD Act, for example, may allow US authorities to compel access to data held by US cloud providers even where the data is physically located outside

the United States. This creates potential conflicts with GDPR provisions restricting transfers of personal data to third countries lacking adequate data protection standards, and with the confidentiality obligations applicable to arbitral proceedings. Effective digital risk management requires careful selection of cloud providers and contractual arrangements ensuring compliance with applicable data protection requirements, including standard contractual clauses or other appropriate transfer mechanisms.

Virtual hearing security requires particular attention in an era when all major arbitral institutions have normalized remote proceedings. Video conferencing platforms used for arbitral hearings process audio and video data of all participants, which may constitute personal data (including biometric data in jurisdictions where voice and facial recognition data are classified as sensitive). Recording of hearings raises issues of consent, purpose limitation, and storage security. Cyber vulnerabilities in commercial video conferencing platforms illustrated by widely publicized security incidents since 2020 demonstrate that standard commercial solutions may be inadequate for the security requirements of confidential arbitral proceedings. Some institutions have adopted dedicated secure hearing platforms with enhanced encryption and access controls, but this practice is far from universal. Legal requirements for the security of personal data processing, under Article 32 of the GDPR, demand that appropriate technical and organizational measures be implemented, but what constitutes appropriate security for arbitral hearings has not been defined in either regulatory guidance or institutional practice.

Artificial intelligence tools are increasingly used in international arbitration for document review, translation, predictive assessment, and case management. These tools process large volumes of documents containing personal data and may engage in automated analysis that affects how evidence is presented and evaluated. The GDPR's restrictions on automated decision-making, under Article 22, apply where processing involves solely automated decision-making that produces legal or similarly significant effects. While most current AI tools are used as advisory aids rather than autonomous decision-makers, the boundaries of this distinction are shifting as AI capabilities advance. Additionally, AI tools may be operated by third-party service providers outside the EU, raising transfer and third-party processor compliance issues. The legal basis for processing personal data through AI tools must be established and documented by controllers, and data protection impact assessments may be required where AI processing is likely to result in high risk to data subjects. These requirements add a layer of regulatory compliance complexity to the use of AI in arbitration that practitioners and institutions need to address systematically.

E. Liability, Accountability, and Ethical Implications

The allocation of liability for confidentiality breaches and data protection violations in digital arbitration is among the most practically significant questions raised by this study. Under civil law principles, liability for breach of confidentiality may arise in contract where parties have agreed to confidentiality obligations in tort

where a duty of care can be established or under specific statutory provisions governing arbitrators' duties. Liability for data protection violations is governed by the GDPR and equivalent national instruments, which impose liability on both data controllers and processors for failure to comply with applicable obligations. The potential for multiple, overlapping liability regimes to apply to a single incident such as a cyber-attack resulting in the disclosure of confidential arbitral materials and personal data creates complex questions about the appropriate allocation of responsibility among parties, institutions, arbitrators, lawyers, and technology service providers.

The accountability framework under the GDPR is based on the principle of accountability, requiring data controllers to demonstrate compliance with applicable data protection principles rather than merely to comply with them passively. In the context of arbitration, this means that institutions and parties acting as controllers must maintain records of their processing activities conduct data protection impact assessments where required, appoint data protection officers where applicable, and implement appropriate technical and organizational security measures. Demonstrating accountability in the digital arbitration context requires that these compliance activities be specifically tailored to the arbitral environment, taking account of the particular types of personal data processed, the specific risks posed by digital proceedings, and the multi-actor nature of arbitral data processing. Existing institutional rules and compliance frameworks do not systematically address these accountability requirements, leaving institutions and parties exposed to regulatory enforcement risk.

The ethical dimensions of digital risk management in arbitration extend beyond legal compliance to questions of professional responsibility, institutional integrity, and the fundamental fairness of arbitral proceedings. Arbitrators owe duties of impartiality, independence, and confidentiality to the parties, and these duties are not diminished by the digital nature of the proceedings. The use of AI tools in arbitral decision-making even in purely advisory capacities raises ethical questions about the transparency of the decision-making process and the ability of parties to understand and challenge AI-generated assessments. Data protection principles of transparency and fairness require that data subjects be informed about the processing of their personal data, creating potential tensions with the confidentiality of arbitral proceedings. Resolving these ethical tensions requires clear institutional guidance and, where appropriate, explicit regulatory intervention establishing rules for the ethical use of digital tools in arbitration.

F. Implications

The findings of this study carry significant implications for arbitral doctrine, institutional design, and legislative reform. At the doctrinal level, the study challenges the traditional assumption that arbitral confidentiality can be adequately guaranteed through party agreement and institutional rules alone. In a digital environment

governed by mandatory data protection legislation with broad extraterritorial reach, confidentiality norms must be designed to operate within and in compliance with the data protection framework rather than in isolation from it. This requires a reconceptualization of arbitral confidentiality as a qualified rather than absolute obligation, shaped by the mandatory requirements of data protection law and subject to the rights of data subjects whose personal information is processed in the course of proceedings.

At the institutional level, the study's findings support a comprehensive review and revision of arbitral rules governing digital proceedings and data protection. Leading institutions have begun this process, but further development is needed. Institutional rules should specify the legal bases for processing personal data in arbitral proceedings, establish procedures for handling data subject access requests in ways that preserve arbitral confidentiality, require the use of secure digital infrastructure meeting defined security standards, address the use of AI tools and the ethical obligations it creates, and establish clear accountability frameworks allocating data protection responsibilities among participants. These rule changes should be developed in consultation with data protection authorities and in alignment with applicable regulatory guidance, ensuring that institutional practice is consistent with legal requirements.

For national legislators in civil law jurisdictions, the study's findings support the adoption of specific provisions addressing the interface between arbitral confidentiality and data protection obligations. Several jurisdictions have recently updated their arbitration legislation including France, Switzerland, and Germany without specifically addressing digital risk management or data protection. Future legislative updates should include clear provisions establishing the relationship between arbitral confidentiality and statutory data protection obligations, including rules for the handling of data subject requests, breach notification procedures, and the use of digital hearing platforms. Uzbekistan, as a developing arbitral seat, has an opportunity to adopt forward-looking legislation that addresses these issues from the outset, positioning itself as a jurisdiction with a clear and coherent legal framework for digital arbitration.

The broader implications of this research extend to the governance of private international law and the regulation of digital dispute resolution systems generally. International commercial arbitration is not an isolated phenomenon; it exists within, and is shaped by, the broader regulatory environment of international trade law, data governance, and digital economy regulation. The principles and solutions developed in the arbitration context may inform governance approaches in other private adjudication systems including international commercial courts, online dispute resolution platforms, and AI-driven mediation systems where similar tensions between confidentiality and data protection arise. The study thus contributes to a broader research agenda on the governance of digital private dispute resolution that has

significant theoretical and practical importance for the future of international commercial law.

The governance implications of the findings extend to the international level, where fragmentation of legal requirements creates systemic risks for parties engaged in multi-jurisdictional commercial arbitration. International commercial arbitration frequently involves parties from multiple legal systems, proceedings administered by institutions in different countries, evidence collected across borders, and awards enforced in jurisdictions whose data protection laws may differ from those applicable at the seat. This multi-jurisdictional dimension means that compliance with data protection obligations in international arbitration requires engagement with multiple regulatory regimes simultaneously. Parties and institutions must map applicable data protection requirements at each stage of the arbitral process from the filing of the request for arbitration through to award enforcement identifying potential conflicts and designing compliance strategies that satisfy the most demanding requirements across the relevant jurisdictions.

The principle of mutual recognition and adequacy decisions under data protection law provides a partial mechanism for facilitating cross-border data transfers in arbitration, but its application to the arbitral context is under-developed. Adequacy decisions recognizing that a third country offers equivalent data protection to the GDPR standard exist for a limited number of countries, and many important arbitral seats are not covered by adequacy determinations. For transfers to countries without adequacy decisions, parties and institutions must rely on alternative transfer mechanisms such as standard contractual clauses, binding corporate rules, or derogations under Article 49 of the GDPR. The use of standard contractual clauses between arbitral participants in different jurisdictions is a practical option that merits further development by international arbitration bodies. Institutional model clauses for cross-border data transfers in arbitration could reduce the transactional cost of establishing compliant transfer arrangements and provide legal certainty for parties and institutions.

The role of national supervisory authorities in the oversight of arbitral data processing has not been systematically addressed in either regulatory or institutional contexts. While supervisory authorities have jurisdiction over data processing activities in their territories, they have not, to date, produced specific guidance on their approach to the arbitration sector. The exercise of supervisory authority over arbitral proceedings including investigations, enforcement actions, and the imposition of corrective measures could in principle conflict with the confidentiality and autonomy of arbitration. The interaction between regulatory oversight and arbitral immunity from national court supervision is a novel legal question that has not been judicially resolved. Proactive engagement between the arbitration community and supervisory authorities through dialogue, consultation, and the development of sector-specific guidance is preferable to litigated disputes about the scope of regulatory jurisdiction

over arbitral proceedings.

Future-proofing arbitral confidentiality and data protection frameworks also requires attention to emerging technologies that are not yet widely deployed but are likely to become significant in the medium term. Blockchain-based evidence management systems, smart contract arbitration platforms, and quantum computing applications in cryptography each present novel governance challenges that the current legal framework is not designed to address. Regulatory sandbox approaches allowing experimentation with new technologies under regulatory supervision before general adoption could provide a mechanism for testing innovative digital arbitration tools while ensuring that confidentiality and data protection standards are maintained. Collaboration between technology developers, arbitral institutions, regulatory authorities, and academic researchers is essential for developing governance frameworks that are technically informed, legally sound, and practically workable.

G. Recommendations

Based on the findings and analysis presented above, this study advances a set of concrete recommendations for regulators, arbitral institutions, and practitioners. The first recommendation is that arbitral institutions revise their rules to include specific, comprehensive provisions on digital data protection, encompassing legal bases for processing, procedures for data subject rights, minimum security standards for digital platforms, data retention and deletion policies, and accountability mechanisms for data protection compliance. The ICC, LCIA, SIAC, and other leading institutions should develop model provisions that can be adapted by smaller institutions and incorporated into national legislative frameworks. The UNCITRAL secretariat should priorities the development of authoritative guidance or model clauses on cybersecurity and data protection in arbitration, building on the preliminary work already undertaken in the digital arbitration space.

The second recommendation concerns the establishment of a harmonized framework for allocating data protection responsibilities among arbitral participants. Regulatory guidance from European data protection authorities either through the European Data Protection Board or through national supervisory authorities in key arbitral seats should address the specific roles of institutions, parties, arbitrators, counsel, and technology service providers as controllers and processors under the GDPR. This guidance should be developed with input from the arbitration community and should provide clear, practical answers to the questions of legal basis, data subject rights, security obligations, and accountability documentation that practitioners currently face without adequate guidance.

The third recommendation concerns the security of digital hearing platforms and cloud-based case management systems. Arbitral institutions and national arbitration associations should develop minimum technical security standards for digital arbitration infrastructure, aligned with existing frameworks such as ISO 27001, the NIST Cybersecurity Framework, and sector-specific guidance for legal services.

These standards should address encryption requirements, access controls, authentication mechanisms, incident response protocols, and vendor security assessment procedures. Compliance with these standards should be a prerequisite for institutional recognition of hearing platforms and case management systems used in arbitral proceedings. Certification schemes, analogous to those used in other highly regulated industries, could provide a mechanism for demonstrating and verifying compliance.

The fourth recommendation is directed at national legislators in civil law jurisdictions. Legislative reform should address the gap between arbitration law and data protection law by introducing specific provisions governing the handling of personal data in arbitral proceedings. These provisions should establish that data protection obligations apply to arbitral processing without displacing the fundamental confidentiality norms of arbitration, clarify the legal bases for processing personal data in arbitration, and provide a mechanism for courts to balance data subject rights against arbitral confidentiality in individual cases. Model legislative language could be developed by UNCITRAL or regional arbitration bodies to promote harmonization across civil law jurisdictions. Uzbekistan and other emerging arbitral seats should seize this opportunity to enact clear and technology-sensitive legislation that provides legal certainty for international commercial parties choosing their jurisdiction as an arbitral seat.

Conclusion

This study has examined the intersection of confidentiality and data protection in international commercial arbitration through the lens of civil law doctrine and digital risk management. The central argument is that the traditional framework of arbitral confidentiality, grounded in party agreement and institutional rules, is insufficient to address the challenges of digital arbitration governed by mandatory data protection legislation. The analysis has demonstrated that civil law systems approach this intersection in diverse ways, creating a fragmented legal landscape that generates uncertainty for parties and institutions operating in the global arbitration market. International frameworks most importantly the GDPR impose obligations on arbitral participants that interact with, and in some cases override, contractual and institutional confidentiality arrangements.

The digital risks associated with modern arbitration cyber intrusions, cloud computing vulnerabilities, virtual hearing security, and AI-related data processing create practical and legal challenges that require systematic institutional and regulatory responses. Existing responses, while positive in direction, are insufficient in scope and coherence. The study has proposed concrete recommendations for institutional rule reform, regulatory guidance, technical security standards, and legislative reform in civil law jurisdictions, grounded in the comparative doctrinal analysis and digital risk assessment presented in the preceding sections. These

recommendations are designed to ensure that arbitral confidentiality remains a meaningful protection in the digital age, compatible with the mandatory requirements of data protection law and capable of inspiring confidence among commercial parties.

The contribution of this research is to demonstrate the necessity of an integrated approach to confidentiality and data protection in digital arbitration one that treats these two frameworks not as competing obligations but as complementary components of a coherent regime for protecting sensitive information in arbitral proceedings. Such integration requires engagement across disciplines, involving arbitration practitioners, data protection specialists, information security experts, and national legislators. It also requires sustained attention from international organizations, particularly UNCITRAL, which has a unique mandate to promote the harmonization of international commercial arbitration law and whose leadership on digital governance issues is urgently needed.

Looking to the future, the governance challenges identified in this study will intensify as arbitration becomes more fully digital, AI capabilities in legal practice advance, and data protection regulation continues to evolve in response to technological change. Emerging issues including the regulation of AI arbitrators, the management of blockchain-based evidence, and the governance of decentralized arbitration platforms will generate new confidentiality and data protection questions that current frameworks are not designed to address. The present study offers a foundation for future research in these areas, grounded in the civil law doctrinal tradition and informed by the practical realities of modern international commercial arbitration. The fundamental challenge is to ensure that the rule of law keeps pace with technological change, preserving the values of privacy, fairness, and accountability that make arbitration a legitimate and trusted form of dispute resolution in the global commercial order.

Bibliography

Born, G. B. (2021). *International commercial arbitration* (3rd ed.). Kluwer Law International.

Bühring-Uhle, C., Kirchhoff, L., & Scherer, M. (2020). *Arbitration and mediation in international business* (3rd ed.). Kluwer Law International.

Cordero-Moss, G. (2019). *International commercial contracts: Applicable sources and enforceability* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781108764650

Kaufmann-Kohler, G., & Rigozzi, A. (2021). *International arbitration: Law and practice in Switzerland* (3rd ed.). Schulthess Verlag.

Lachmann, J. P. (2022). Data protection in international arbitration: GDPR obligations and practical guidance. *Journal of International Arbitration*, *39*(2), 145–178. https://doi.org/10.54648/JOIA2022009

London Court of International Arbitration. (2020). *LCIA arbitration rules 2020*. LCIA. https://www.lcia.org/Dispute_Resolution_Services/lcia-arbitration-rules-2020.aspx

Moses, M. L. (2017). *The principles and practice of international commercial arbitration* (3rd ed.). Cambridge University Press. https://doi.org/10.1017/9781316795576

Mourre, A. (2021). Confidentiality and transparency in international arbitration: The civil law perspective. *Arbitration International*, *37*(1), 1–28. https://doi.org/10.1093/arbint/aiab001

Rosenthal, M. (2020). Professional secrecy and data protection in French arbitration law. *Revue de l'Arbitrage*, *2020*(3), 789–812.

Viscasillas, P. P. (2020). Artificial intelligence in international commercial arbitration: The use of AI tools and their legal implications. *Journal of International Dispute Settlement*, *11*(4), 563–589. https://doi.org/10.1093/jnlids/idaa024

Wahab, M. S. A. (2023). Cybersecurity in international arbitration: Risks, obligations, and institutional responses. *Transnational Dispute Management*, *20*(1), 1–35.