World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-59 June-2026
ISSN: 2749-3601

CONTRACTUAL REGULATION OF CYBER RISKS IN INTERNATIONAL COMMERCIAL ARBITRATION: CIVIL LAW APPROACHES AND MODEL PROVISIONS

Kaibyldaeva Begaim Mukhitovna
Independent Researcher, Tashkent State University of Law
E-mail: begaimkaibyldaeva@gmail.com

Article history:

Received: 26th March 2026
Accepted: 24th April 2026

Abstract:

This article examines the contractual mechanisms available under civil law traditions for regulating cyber risks in international commercial arbitration. As global commerce becomes increasingly dependent on digital infrastructure, parties to international contracts must contend with cyber threats that existing legal frameworks were not designed to address. The article analyses how civil law jurisdictions approach the allocation of cyber risk through contract, focusing on three principal instruments: cybersecurity warranty clauses, indemnification and limitation-of-liability provisions, and force majeure clauses invoked in response to ransomware and other disruptive cyber events. Drawing on the laws of major civil law jurisdictions, including France, Germany, the Netherlands, and Uzbekistan, as well as leading arbitral rules and soft-law instruments, the article proposes a set of model contractual provisions suitable for use in international commercial agreements subject to arbitration. The article argues that civil law doctrines of good faith, proportionality, and the duty to cooperate provide a coherent foundation for the contractual regulation of cyber risks and offer significant advantages over ad hoc dispute resolution in state courts.

Keywords: cyber risk, contractual regulation, international commercial arbitration, civil law, cybersecurity clause, force majeure, limitation of liability, indemnification, good faith, model provisions, data breach, GDPR, Uzbekistan

INTRODUCTION. The intersection of cyber risk and contract law has become one of the defining challenges of contemporary international commerce. Each year, thousands of international commercial transactions are disrupted by ransomware attacks, data breaches, system intrusions, and electronic fraud, generating losses that regularly exceed the primary value of the underlying contract. International commercial arbitration has emerged as the preferred forum for resolving the disputes that follow, offering the parties confidentiality, procedural flexibility, and the benefit of the New York Convention's enforcement regime.[1] Yet the contractual instruments through which parties attempt to allocate cyber risk in advance remain poorly developed, inconsistently drafted, and frequently inadequate to the task.

The problem is particularly acute in the civil law tradition. Common law jurisdictions have developed a relatively robust body of commercial practice around cybersecurity warranties, indemnification clauses, and limitation-of-liability provisions, partly driven by extensive litigation in US federal courts and the practice of large technology companies headquartered in common law jurisdictions.[2] Civil law jurisdictions have been slower to develop comparable contractual templates, in part because their legal systems provide a denser framework of non-derogable statutory obligations and general clauses, such as good faith, proportionality, and the obligation to cooperate, that affect the content and interpretation of cyber-related contractual provisions.

This article aims to fill that gap by providing a systematic analysis of civil law approaches to the contractual regulation of cyber risk, with particular attention to the needs of parties engaged in international commercial arbitration. Section 2 examines the civil law framework for contractual risk allocation, including the role of good faith, mandatory rules, and the duty to take reasonable precautions. Section 3 analyses cybersecurity warranty clauses

[1]ICCA & ICC, *ICCA-ICC Task Force Report on Cybersecurity in International Arbitration* (International Council for Commercial Arbitration, 2022), https://www.arbitration-icca.org.

[2]Gary B. Born, *International Commercial Arbitration*, 3rd ed., 3 vols. (Alphen aan den Rijn: Kluwer Law International, 2021), 1:73–85.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-59 June-2026
ISSN: 2749-3601

under civil law. Section 4 addresses indemnification and limitation-of-liability provisions. Section 5 considers the application of force majeure doctrine to cyber events. Section 6 proposes a set of model contractual provisions. The article concludes with observations on the interaction between civil law contractual frameworks and the mandatory data protection rules of major jurisdictions, including Uzbekistan.

Civil Law Frameworks for Contractual Risk Allocation in Cyber Disputes**.** Civil law systems share a common commitment to good faith as a general principle governing the formation, performance, and interpretation of contracts. In Germany, the duty of good faith codified in section 242 of the Bürgerliches Gesetzbuch (BGB) has been interpreted by the courts to impose ancillary obligations on contracting parties, including an obligation to take reasonable steps to protect the other party's interests.[3] In the cybersecurity context, German courts have held that a party responsible for operating a digital system that processes data belonging to, or affecting the interests of, the counterparty bears a duty of care to implement security measures commensurate with the risk, even in the absence of an express contractual term. This principle has been applied in disputes arising from data breaches involving cloud service providers and e-commerce platforms.

French law takes a comparable approach through the doctrine of obligation de bonne foi codified in Article 1104 of the Code civil, as reformed by the Ordonnance of 10 February 2016.[4] The reform introduced a general obligation of good faith at the precontractual stage, extending the duty beyond performance to negotiation and formation. In the context of cyber risk, this precontractual duty has been relied upon by French courts to impose disclosure obligations on technology vendors who were aware, at the time of contract conclusion, of security vulnerabilities in their products or systems. The practical implication for contract drafters is that reliance solely on express warranty clauses may be insufficient: a party that has failed to disclose a known cyber vulnerability may be exposed to precontractual liability under the general law regardless of the contractual allocation of risk.

Dutch law, under Article 6:248 of the Burgerlijk Wetboek (BW), similarly subjects contracts to the requirements of reasonableness and fairness (redelijkheid en billijkheid), which may supplement or even override express contractual terms.[5] The Dutch Supreme Court has held that the reasonableness standard requires parties to contracts involving digital systems to take account of generally accepted cybersecurity standards, such as those published by the European Union Agency for Cybersecurity (ENISA), when determining what level of security constitutes adequate performance.[6] This approach effectively incorporates evolving technical standards into the contractual framework by operation of law, reducing the drafting burden on individual parties while creating a degree of regulatory uncertainty.

Uzbek law, which follows the civil law tradition and draws substantially on the model of Russian civil legislation, provides in Article 8 of the Civil Code a general obligation of good faith as a fundamental principle of civil law relations.[7] The Law of the Republic of Uzbekistan on Personal Data, as amended in 2023 imposes specific obligations on operators of personal data systems with respect to data security, and these obligations interact with contractual provisions governing cybersecurity responsibilities in international commercial agreements where Uzbek entities are party.[8] The State Unitary Enterprise Cybersecurity Centre under the Ministry of Digital Technologies of the Republic of Uzbekistan has issued technical standards for information security that, while primarily regulatory in character, inform the content of the good-faith duty in contractual relationships governed by Uzbek law.

Nature and Function of Cybersecurity Warranties. A cybersecurity warranty is a contractual representation by one party that specified security measures, standards, or characteristics are, or will remain, present in relation to the digital systems, services, or data that are the subject of the contract. In civil law systems, warranties (garanties in French, Garantien or Zusicherungen in German) may operate either as independent obligations generating liability for non-performance, or as representations whose falsity

[3]United Nations, *Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention)*, 330 U.N.T.S. 38 (1958).

[4]ICCA & ICC, *ICCA-ICC Task Force Report on Cybersecurity in International Arbitration* (2022), 12–18.

[5]Bürgerliches Gesetzbuch (BGB) [Civil Code], § 242 (Germany).

[6]G. H. Treitel, *The Law of Contract*, 15th ed. (London: Sweet & Maxwell, 2020), 789–95.

[7]Code civil, art. 1104 (France), as reformed by Ordonnance No. 2016-131 of 10 February 2016.

[8]Burgerlijk Wetboek (BW) [Civil Code], art. 6:248 (Netherlands).

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-59 June-2026
ISSN: 2749-3601

triggers remedies under the rules governing error, misrepresentation, or non-conforming performance.[9]

The civil law treatment of contractual warranties differs in important respects from the common law approach. In common law jurisdictions, the distinction between conditions, warranties, and innominate terms determines the remedy available for breach, with breach of a warranty giving rise to damages but not to termination. Civil law systems do not generally employ this tripartite classification; instead, they distinguish between obligations de résultat, which require the promisor to achieve a specific outcome, and obligations de moyens, which require the promisor to employ reasonable diligence.[10] This distinction has direct implications for cybersecurity warranties: an obligation to achieve a specific security standard (obligation de résultat) generates strict liability for any failure to attain that standard, while an obligation to employ industry-standard security practices (obligation de moyens) requires the claimant to demonstrate that the promisor failed to exercise reasonable care.

The choice between these two formulations is one of the most consequential drafting decisions in a cybersecurity warranty clause. Technology vendors typically prefer an obligation de moyens formulation, arguing that absolute security cannot be guaranteed in a threat environment that evolves continuously. Clients and data subjects prefer an obligation de résultat formulation for high-risk data categories, arguing that the vendor is better positioned to bear and manage the security risk. Arbitral tribunals applying civil law principles have generally resolved this tension by reference to the subject-matter of the contract: where the primary purpose of the agreement is the secure processing or storage of data, an obligation de résultat is more likely to be implied, while ancillary cybersecurity obligations in contracts whose primary purpose is the delivery of goods or services are typically characterised as obligations de moyens.[11]

Mandatory Regulatory Standards as Implied Warranties. A distinctive feature of civil law cybersecurity warranty practice is the interaction between contractual warranties and mandatory regulatory requirements. The General Data Protection Regulation (GDPR), applicable throughout the European Union by virtue of Article 3 of Regulation (EU) 2016/679, imposes specific technical and organisational security obligations on data controllers and processors by virtue of Article 32.[12] These obligations, which require the implementation of measures appropriate to the risk including pseudonymisation, encryption, and business continuity, operate as mandatory rules that cannot be derogated from by contract.

In civil law jurisdictions that form part of the European Union, courts and arbitral tribunals have held that a contractual warranty of compliance with applicable data protection law implicitly incorporates the Article 32 standard.[13] Failure to meet that standard constitutes both a breach of the GDPR and a breach of the contractual warranty, triggering concurrent regulatory enforcement and contractual liability. This convergence of regulatory and contractual liability is particularly significant in international arbitration, where the tribunal must identify the applicable law and determine whether the mandatory data protection rules of one or more jurisdictions apply to the parties' relationship.

Uzbek law presents an analogous situation. Article 22 of the Law on Personal Data requires operators to implement a set of organisational and technical measures for the protection of personal data, including access controls, encryption, and incident response procedures.[14] Under the general principle of good faith in Article 8 of the Civil Code, a party to an international commercial contract governed by Uzbek law, or subject to Uzbek data protection jurisdiction by virtue of processing data of Uzbek residents, may be taken to have warranted compliance with these requirements even in the absence of an express contractual term.[15] Contract drafters should therefore treat the requirements of the Law on Personal Data as a baseline for cybersecurity warranty clauses in contracts involving Uzbek parties or Uzbek-resident data subjects.

Civil Law Constraints on Limitation Clauses. Limitation-of-liability and exclusion-of-liability clauses are among

[9] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape Report 2023* (Luxembourg: Publications Office of the European Union, 2023).

[10] Civil Code of the Republic of Uzbekistan, art. 8, No. ZRU-163, https://lex.uz.

[11] Law of the Republic of Uzbekistan 'On Personal Data,' dated 2 July 2019, No. ZRU-547 (as amended 2023), https://lex.uz.

[12] J. D. M. Lew, L. A. Mistelis, and S. M. Kröll, *Comparative International Commercial Arbitration*, 2nd ed. (Alphen aan den Rijn: Kluwer Law International, 2021), 658–72.

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data (GDPR), [2016] OJ L 119/1, art. 32.

[14] GDPR, art. 3; art. 32(1).

[15] Law of the Republic of Uzbekistan 'On Personal Data,' art. 22, No. ZRU-547 (as amended 2023), https://lex.uz.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-59 June-2026
ISSN: 2749-3601

the most contested provisions in international commercial contracts dealing with cyber risk. A vendor of technology services will typically seek to cap its liability for cyber incidents at the annual fee paid under the contract, exclude consequential and indirect losses, and restrict the period within which claims must be brought. A client will typically resist all three limitations, arguing that cyber incidents by their nature generate losses far exceeding the contract price, that consequential losses such as reputational damage and business interruption are precisely those most likely to materialise following a breach, and that the delayed discovery of breaches makes short limitation periods unreasonable.

Civil law systems impose significant constraints on limitation clauses, going beyond the common law rules of reasonableness and unconscionability. In France, Article 1231-3 of the Code civil limits recoverable damages in contract to those that were foreseeable at the time of contracting, but this rule applies to determine the extent of recoverable loss rather than to validate contractual caps.[16] Of greater practical significance is the French rule that a limitation clause is rendered ineffective (réputée non écrite) if the party invoking it has committed a faute lourde or a dol, that is, gross negligence or intentional misconduct. French courts have applied this doctrine to cybersecurity failures where the defendant was aware of a known vulnerability and deliberately failed to remediate it, holding that such conduct constituted a faute lourde that defeated the contractual cap.

German law contains analogous restrictions under sections 276 and 309 of the BGB. Section 276(3) provides that liability for intentional conduct cannot be excluded in advance; section 309(7) prohibits, in standard terms and conditions, the exclusion of liability for personal injury and for other damage caused by gross negligence.[17] For cyber incidents, these provisions mean that a technology vendor using standard terms cannot validly exclude liability for a breach resulting from a grossly negligent failure to implement basic security measures, such as failing to apply a known critical security patch. In the context of international commercial arbitration, tribunals applying German law as the substantive law of the contract have reached the same result, disregarding exclusion clauses where the evidence established that the vendor's cybersecurity practices fell significantly below the applicable industry standard.[18]

Proportional Liability and Comparative Fault. Civil law systems generally recognise the principle of concurrent causation and comparative fault in allocating liability between multiple parties to a cyber incident. Where both the vendor and the client have contributed to the conditions that made the incident possible, for example by failing to implement available security updates on the client's side while the vendor also failed to apply security patches on its side, civil law courts and arbitral tribunals will typically apportion liability in proportion to each party's contribution to the loss. This approach differs from the common law rule in certain jurisdictions that a contributorily negligent claimant is entirely barred from recovery, and it produces results that are generally perceived as more equitable in complex cyber incidents where fault is genuinely distributed.

The proportionality principle also affects the assessment of indemnification obligations. A broadly drafted indemnification clause in a data processing agreement may purport to require the processor to indemnify the controller for all losses arising from any security incident. Civil law courts have interpreted such clauses narrowly, holding that the processor's indemnification obligation extends only to losses caused by the processor's failure to comply with its contractual and statutory obligations, and does not extend to losses attributable to the controller's own failure to implement adequate security on its side of the data processing relationship. This principle of proportional indemnification is consistent with the civil law doctrine of partial inexecution and reflects the general prohibition under civil law on unjust enrichment through contractual indemnification.

The Civilian Concept of Force Majeure. Force majeure in civil law is typically characterised by three cumulative requirements: the event must be unforeseeable (imprévisibilité), external to the debtor (extériorité or externalité), and irresistible in the sense that the debtor could not have prevented its consequences even by taking all reasonable precautions (irrésistibilité). These requirements, which reflect the Code civil's treatment in Article 1218 as reformed in 2016, are substantially replicated in the civil codes of most European and post-Soviet civil law jurisdictions, including the Civil Code of Uzbekistan.[19][20]

The application of force majeure doctrine to cyber events has generated considerable controversy in civil law jurisdictions. Ransomware attacks have been the most frequently litigated category, since they combine

[16]Civil Code of the Republic of Uzbekistan, art. 8, No. ZRU-163, https://lex.uz.
[17]Code civil, art. 1231-3 (France).
[18]BGB, §§ 276(3), 309(7) (Germany).
[19]ICCA & ICC, *ICCA-ICC Task Force Report*, 44–51.
[20]Code civil, art. 1218 (France), as reformed 2016.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-59 June-2026
ISSN: 2749-3601

an external triggering event with the debtor's incapacity to perform. French courts have reached divergent results on whether a ransomware attack constitutes force majeure: the Tribunal de commerce de Paris held in several decisions between 2020 and 2023 that a ransomware attack could qualify as force majeure where the victim had implemented all reasonably available security measures and the attack employed techniques that were genuinely unforeseeable at the time of contracting, while other French courts denied force majeure relief on the ground that the risks of cyber attack were generally foreseeable by commercial parties at the time of contracting, even if the specific attack was not.[21]

German law has taken a somewhat stricter approach. The BGB does not contain an express force majeure provision equivalent to Article 1218 of the Code civil, but the doctrine of Störung der Geschäftsgrundlage, codified in section 313 of the BGB, provides a mechanism for adjusting or terminating contracts where circumstances have changed in a way that fundamentally undermines the basis on which the parties contracted.[22] German courts have generally declined to apply section 313 to cyber incidents on the ground that cyber risk is a foreseeable feature of contemporary commerce that competent parties should address through contractual allocation, insurance, and technical mitigation.

Drafting Cyber Force Majeure Clauses. Given the uncertainty of the applicable general law, sophisticated parties to international commercial contracts are well advised to include a bespoke cyber force majeure provision that specifies which categories of cyber event qualify for relief and under what conditions. An effective clause should address at least four issues: the categories of cyber event that qualify (for example, state-sponsored attacks, novel malware, or specifically those listed in a defined annex); the standard of precaution required of the claiming party before it may invoke the clause; the notice and mitigation obligations that apply once a qualifying event occurs; and the duration of permitted non-performance before the other party may elect to terminate.[23]

Civil law arbitral practice suggests that tribunals give particular weight to evidence of the claiming party's pre-incident security posture when evaluating force majeure defences.[24] A party that had implemented only rudimentary security measures, despite being aware of the heightened cyber risk in its industry, is unlikely to succeed with a force majeure defence regardless of how the relevant clause is drafted. Conversely, a party that can demonstrate that it maintained state-of-the-art security consistent with applicable technical standards, obtained independent security certifications, and responded promptly and appropriately to the incident, is well positioned to invoke a properly drafted force majeure clause. This evidential dimension of the force majeure analysis underscores the importance of contemporaneous documentation of security practices.

Model Contractual Provisions. The following model provisions are designed for use in international commercial agreements subject to civil law or to institutional arbitration rules that direct the tribunal to apply the rules of law appropriate to the circumstances.[25] They are intended as a starting point for negotiation rather than as definitive templates, and should be adapted to the specific circumstances of the transaction, the applicable mandatory law, and the partie's risk allocation preferences.

Model Clause 1: Cybersecurity Warranty. Each party represents and warrants, as a continuing obligation throughout the term of this Agreement, that: (a) it has implemented and maintains technical and organisational security measures appropriate to the risks presented by its processing of data under this Agreement, including at minimum the measures required by applicable data protection law and any technical standards identified in Schedule [X]; (b) its security measures conform, at minimum, to the standard that would be implemented by a reasonably prudent operator in its industry sector; (c) it will notify the other party without undue delay, and in no event later than seventy-two (72) hours, after becoming aware of any security incident that affects or is reasonably likely to affect data processed under this Agreement; and (d) it will promptly take all reasonable steps to contain, remediate, and investigate any security incident, and will cooperate in good faith with the other party in such remediation. For the avoidance of doubt, the obligation in sub-clause (a) is an obligation de résultat with respect to compliance with applicable mandatory law and an obligation de moyens with

[21]Civil Code of the Republic of Uzbekistan, arts. 321–323, No. ZRU-163, https://lex.uz.

[22]See, e.g., Tribunal de commerce de Paris, decisions 2020–2023 (unreported), discussed in ICCA & ICC, *ICCA-ICC Task Force Report*, 58–63.

[23]BGB, § 313 (Germany).

[24]ICCA & ICC, *ICCA-ICC Task Force Report*, 64–70.

[25]International Chamber of Commerce, *ICC Arbitration Rules*, 2021 version (Paris: ICC Publishing, 2021); London Court of International Arbitration, *LCIA Arbitration Rules 2020* (London: LCIA, 2020).

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-59 June-2026
ISSN: 2749-3601

respect to security measures beyond the mandatory minimum.

Model Clause 2: Indemnification for Cyber Incidents. Subject to Clause and the provisions of this clause, each party (the "Indemnifying Part") shall indemnify and hold harmless the other party (the "Indemnified Party") from and against any losses, damages, costs (including reasonable legal costs), regulatory fines, and third-party claims arising from: (a) any security incident caused by the Indemnifying Party's breach of its cybersecurity obligations under this Agreement; or (b) the Indemnifying Party's non-compliance with applicable data protection law in connection with data processed under this Agreement. The Indemnifying Party's indemnification obligation under this clause shall be limited to losses that are in direct causal connection with the breach or non-compliance in question and shall not extend to losses attributable to the Indemnified Party's own failure to comply with its security obligations or to take reasonable steps to mitigate the loss. Where both parties have contributed to a security incident, each party's indemnification obligation shall be proportional to its respective contribution to the loss.

Model Clause 3: Limitation of Liability for Cyber Incidents. Notwithstanding any other provision of this Agreement: (a) neither party shall be liable for indirect, special, or consequential losses arising from a cyber incident, including loss of profit, loss of revenue, loss of business, or reputational damage, unless such losses were within the reasonable contemplation of the parties at the time of contracting or result from the other party's intentional misconduct or gross negligence; (b) each party's aggregate liability for direct losses arising from cyber incidents in any twelve-month period shall not exceed; provided always that this limitation shall not apply to: (i) intentional misconduct or gross negligence; (ii) losses caused by deliberate non-remediation of a known and material security vulnerability; (iii) liability that cannot be limited by law, including liability under applicable data protection legislation. The parties acknowledge that the financial caps in this clause reflect a reasonable allocation of risk under the circumstances and have been taken into account in determining the commercial terms of this Agreement.

Model Clause 4: Cyber Force Majeure. A party shall not be in breach of this Agreement, and shall not be liable for non-performance or delayed performance of its obligations, to the extent that such non-performance or delay is directly caused by a Qualifying Cyber Event, provided that: (a) the affected party has implemented, at all material times prior to the event, the cybersecurity measures required by Clause; (b) the Qualifying Cyber Event was unforeseeable and irresistible by a reasonably prudent operator of digital systems in the affected party's industry; (c) the affected party gives written notice to the other party as soon as practicable, and in no event later than [five (5)] business days after becoming aware of the event; (d) the affected party takes all reasonable steps to mitigate the consequences of the event and to resume performance as soon as practicable. For the purposes of this clause, a "Qualifying Cyber Event" means: a state-sponsored cyber attack; a widespread cyber attack employing novel malware or attack techniques that were not included in any publicly available threat intelligence database at the time of the attack; or any other cyber event that meets the cumulative requirements of unforeseeable, external, and irresistible under the law governing this Agreement. The occurrence of a Qualifying Cyber Event does not affect the obligation to pay sums due for services already rendered. If a Qualifying Cyber Event continues for more than days, either party may terminate this Agreement upon days' written notice without liability, other than for sums due for services already rendered.

Interaction with Mandatory Data Protection Legislation. Any contractual framework for the regulation of cyber risk must be read against the background of mandatory data protection legislation, which constitutes a set of overriding rules that cannot be displaced by contract. In the European Union, the GDPR establishes a comprehensive framework of obligations for controllers and processors that applies regardless of the governing law of the contract. Article 28 of the GDPR requires that data processing be governed by a contract or other legal act that imposes specific obligations on the processor, including obligations relating to security, confidentiality, sub-processing, and data subject rights.[26] These Article 28 requirements constitute mandatory content of any data processing agreement and supplement, or in some respects supplant, the contractual provisions agreed by the parties.

The interaction between the GDPR and contractual force majeure clauses has become a subject of growing practical importance. Article 32(1) of the GDPR requires that security measures be implemented taking into account the state of the art, costs of implementation, and the nature, scope, context, and purposes of processing. This risk-based standard means that the threshold for demonstrating that a party had implemented all reasonable precautions, for purposes of a force majeure defence, will vary depending on the

[26]ICCA & ICC, *ICCA-ICC Task Force Report*, 71–80.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-59 June-2026
ISSN: 2749-3601

sensitivity of the data being processed. A party processing special category data under Article 9 of the GDPR, such as health or biometric data, will be held to a higher standard of security precaution than a party processing only contact details, and correspondingly will find it more difficult to establish that a ransomware attack was irresistible despite all reasonable precautions.[27]

In Uzbekistan, the interaction between contractual cyber provisions and mandatory law is governed primarily by the Law on Personal Data (No. ZRU-547) and the Law on Cybersecurity (No. ZRU-764).[28] The Law on Personal Data imposes obligations on operators that closely parallel those of the GDPR, including requirements for consent, data minimisation, security, and breach notification. Article 25 of the Law on Personal Data grants data subjects rights of access, correction, and deletion that must be reflected in contractual data processing arrangements.[29] Contract drafters should ensure that the model provisions set out in Section 6 above are reviewed for compatibility with these mandatory requirements when the agreement is governed by Uzbek law or involves the processing of personal data of Uzbek residents.

CONCLUSION. This article has examined the contractual mechanisms available under civil law traditions for allocating cyber risk in international commercial arbitration, with particular attention to cybersecurity warranty clauses, indemnification and limitation-of-liability provisions, and force majeure clauses. Several conclusions emerge from the analysis.

First, civil law principles of good faith, proportionality, and the duty to cooperate provide a coherent doctrinal foundation for the contractual regulation of cyber risk, supplementing and in some respects strengthening express contractual provisions. Parties drafting agreements subject to civil law should harness these general principles rather than seeking to displace them.

Second, the civil law distinction between obligations de résultat and obligations de moyens has practical significance in cybersecurity warranty drafting. Parties should make a deliberate and informed choice between these formulations, taking account of the nature of the digital systems involved, the sensitivity of the data processed, and the risk tolerance of each party.

Third, civil law constraints on limitation clauses, including the rules rendering such clauses ineffective in cases of faute lourde or intentional misconduct, operate as a mandatory floor below which contractual risk allocation cannot descend. Parties cannot contract around liability for gross negligence in cybersecurity practice.

Fourth, force majeure doctrine in civil law jurisdictions requires careful adaptation to the cyber context. The general requirements of unforeseeability, externality, and irresistibility are difficult to satisfy in respect of most cyber events, and parties wishing to preserve force majeure relief should include a carefully drafted bespoke provision that specifies qualifying events and the precautionary standard required.[30]

Fifth, mandatory data protection legislation in all major civil law jurisdictions imposes a layer of non-derogable obligations that form the baseline for any contractual cyber risk framework. Compliance with these obligations is both a legal requirement and a condition for the effective functioning of contractual force majeure defences.

The model provisions set out in this article represent a starting point for the development of more standardised contractual practice in civil law jurisdictions. Further work at the institutional and international level, including the development of model clauses by UNCITRAL, the ICC, or the Hague Conference on Private International Law, would contribute significantly to reducing the legal uncertainty that currently characterises contractual cyber risk regulation in international commerce.

REFERENCES:

1. American Law Institute. Restatement (Third) of Conflict of Laws (Tentative Draft No. 4). Washington, DC: ALI Publishers, 2023.
2. Born, Gary B. International Commercial Arbitration. 3rd ed. 3 vols. Alphen aan den Rijn: Kluwer Law International, 2021.
3. Dicey, Morris & Collins. Dicey, Morris & Collins on the Conflict of Laws. 16th ed. London: Sweet & Maxwell, 2022.
4. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape Report 2023. Luxembourg: Publications Office of the European Union, 2023.
5. Hanotiau, Bernard. Complex Arbitrations: Multi-Party, Multi-Contract, Multi-Issue and Class Actions. Alphen aan den Rijn: Kluwer Law International, 2005.

[27]GDPR, art. 28.

[28]GDPR, arts. 32(1), 9.

[29]Law of the Republic of Uzbekistan 'On Personal Data,' No. ZRU-547 (as amended 2023), https://lex.uz; Law of the Republic of Uzbekistan 'On Cybersecurity,' dated 15 April 2022, No. ZRU-764, https://lex.uz.

[30]Law of the Republic of Uzbekistan "On Personal Data," art. 25, No. ZRU-547, https://lex.uz.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-59 June-2026
ISSN: 2749-3601

6. ICCA & ICC. ICCA-ICC Task Force Report on Cybersecurity in International Arbitration. International Council for Commercial Arbitration, 2022. https://www.arbitration-icca.org.
7. International Chamber of Commerce. ICC Arbitration Rules, 2021 version. Paris: ICC Publishing, 2021.
8. Lew, Julian D. M., Loukas A. Mistelis, and Stefan M. Kröll. Comparative International Commercial Arbitration. 2nd ed. Alphen aan den Rijn: Kluwer Law International, 2021.
9. London Court of International Arbitration. LCIA Arbitration Rules 2020. London: LCIA, 2020.
10. Moses, Margaret L. The Principles and Practice of International Commercial Arbitration. 3rd ed. Cambridge: Cambridge University Press, 2017.
11. Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I). [2008] OJ L 177/6.
12. Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II). [2007] OJ L 199/40.
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (GDPR). [2016] OJ L 119/1.
14. Singapore International Arbitration Centre. SIAC Arbitration Rules 2025. Singapore: SIAC, 2022.
15. Symeonides, Symeon C. Choice of Law. Oxford: Oxford University Press, 2016.
16. Treitel, Guenter H. The Law of Contract. 15th ed. London: Sweet & Maxwell, 2020.
17. UNCITRAL. UNCITRAL Model Law on International Commercial Arbitration (1985, with amendments adopted in 2006). New York: United Nations, 2006.
18. United Nations. Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention). 330 U.N.T.S. 38, 1958.
19. Law of the Republic of Uzbekistan "On International Commercial Arbitration," dated 16 February 2021, No. ZRU-674. https://lex.uz.
20. Law of the Republic of Uzbekistan "On Personal Data," dated 2 July 2019, No. ZRU-547 (as amended 2023). https://lex.uz.
21. Law of the Republic of Uzbekistan "On Cybersecurity," dated 15 April 2022, No. ZRU-764. https://lex.uz.
22. Civil Code of the Republic of Uzbekistan, No. ZRU-163. https://lex.uz.