INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 4 | Issue 5 | 2025 Art. 10

Lawful Bases for Data Processing in International Arbitration: A Comparative Mapping of Global Approaches

Md Lutfur Rahman
Research Scholar,
Faculty of Legal Studies,
South Asian University, New Delhi

Recommended Citation
Md Lutfur Rahman, *Lawful Bases for Data Processing in International Arbitration: A Comparative Mapping of Global Approaches*, 4 IJHRLR 131-155 (2025).
Available at www.humanrightlawreview.in/archives/.

Lawful Bases for Data Processing in International Arbitration: A Comparative Mapping of Global Approaches

Md Lutfur Rahman
Research Scholar,
Faculty of Legal Studies,
South Asian University, New Delhi

ABSTRACT

As international arbitration increasingly relies on digital communication and data exchange across borders, understanding the lawful bases for such processing under various data protection laws has become a pressing concern. This article compares fifteen major data protection regimes—including those of the EU, UK, Switzerland, China, India, Singapore, Japan, South Korea, Brazil, South Africa, UAE, Australia, Russia, Canada, and California—to identify lawful bases for personal data processing relevant to arbitration. The analysis reveals that while 'consent' remains the most common ground for lawful processing, it is largely impractical in arbitral contexts due to the multiplicity of data subjects and the procedural structure of arbitration. Contractual necessity and legal obligation are similarly limited in scope. 'Legitimate interest' emerges as the most appropriate ground for arbitration-related processing, recognised directly or indirectly in thirteen jurisdictions. Brazil and Russia expressly include arbitration within their frameworks, while Switzerland's principle-based approach similarly accommodates it. The article concludes that harmonisation of data protection compliance in international arbitration is achievable by recognising and justifying arbitral data processing as a legitimate interest, balancing data protection obligations with procedural efficiency.

ABSTRACT

International arbitration, data protection, lawful basis, global harmonisation.

1. INTRODUCTION

The rapid growth of information and communication technology (ICT) has transformed traditional data processing systems into autonomous systems. As data becomes a core asset in the global economy, concerns over its misuse have intensified and given rise to robust data protection frameworks across jurisdictions.[1] Data protection refers to the legal protection afforded to natural persons, commonly referred to as data subjects, against the risks posed by the processing of personal data.[2] This protection is anchored in a framework of legal and non-legal measures designed to safeguard individuals from harm arising from the collection, storage, use, disclosure, or other forms of processing of information concerning them.[3] As Bygrave observes, data protection encompasses a coherent set of principles that regulate the processing of personal information, including both automated and manual operations.[4]

At present, 144 countries have enacted comprehensive national legislation for data protection.[5] In the EU, data protection is recognised as a fundamental right and governed by the General Data Protection Regulation (GDPR),[6] which establishes a uniform framework while granting member states a limited scope for supplementary rules. The GDPR permits the transfer of personal data outside the European Economic Area (EEA) only if the European Commission has issued an adequacy decision for the recipient country or if appropriate safeguards are in place under the Regulation.[7] To date, only ten jurisdictions have secured adequacy, mainly by updating their data protection laws to align with the GDPR and maintain equivalence.[8]

---

[1] Lee A. Bygrave, 'Privacy and data protection in an international perspective' (2010) 56 Scandinavian studies in law 165, 167.
[2] Anneliese Roos, 'Core principles of data protection law' (2006) 39 Comparative and International Law Journal of Southern Africa 102, 104.
[3] see, Frits Hondius, *Emerging Data Protection in Europe* (North-Holland Publishing Co and American Elsevier Publishing Co 1975) 1.
[4] Lee A. Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002) 21– 22.
[5] Aly Apacible-Bernardo and Kayla Bushey, 'Data protection and privacy laws now in effect in 144 countries' (IAPP, 6 March 2023) <https://iapp.org/news/a/data-protection-and-privacy-laws-now-in-effect-in-144-countries> accessed 22 September 2025.
[6] Charter of Fundamental Rights of the European Union [2000] OJ C 364/1 art 8.
[7] 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 art 44–46 (GDPR).
[8] European Commission, 'Adequacy Decisions'

Furthermore, many countries have adopted comprehensive frameworks inspired by the GDPR, but tailored to their own domestic priorities and needs. For instance, India's Digital Personal Data Protection Act, 2023, incorporates core GDPR principles while providing broad exemptions for government agencies and empowering the central government to restrict transfers to designated countries.[9] China's Personal Information Protection Law (PIPL) incorporates a robust national security dimension, mandating government assessments and imposing local storage and processing requirements on sensitive and critical data.[10] The United States, in contrast, maintains a fragmented sectoral and state-level approach to data protection while embedding national security concerns through restrictions on transfers to 'countries of concern' identified by the Department of Justice.

Despite fragmented regulatory regimes, the primary principle of data protection laws is that personal data must be processed lawfully and fairly.[11] GDPR states that personal data should be 'processed lawfully, fairly, and in a transparent manner in relation to the data subject.'[12] Recital 40 of the GDPR states that personal data should be processed based on the explicit consent of the data subject or on other legitimate grounds to ensure lawful data processing.[13] This means that to process personal data, there must be a lawful basis for processing to be considered lawful and fair.

Like other sectors, international arbitration has also incorporated ICT to facilitate the resolution of cross-border disputes. Electronic data transmission is now standard at every stage of the arbitral process, delivering benefits such as reduced costs, faster timelines, and improved accessibility. However, this digital shift has also intensified concerns about data protection and cybersecurity. Because arbitration is inherently transnational and involves parties, counsel, and institutions situated in multiple jurisdictions. It depends on the continuous exchange of personal and case-related data across borders. This, in turn, exposes proceedings to a complex web of mandatory data protection obligations.

<https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 11 September 2025.

[9] Digital Personal Data Protection Act 2023 (India).

[10] Personal Information Protection Law of the People's Republic of China (adopted 20 August 2021, effective 1 November 2021).

[11] GDPR (n 6) art 51(1).

[12] Ibid art 5 (1)(a).

[13] Ibid re 40.

The challenge lies in the fragmentation of data protection regimes. While some jurisdictions, such as the EU, adopt a rights-based model anchored in the GDPR, others, like China or India, follow state-centric or hybrid approaches. As a result, a single arbitral proceeding may simultaneously trigger multiple and potentially conflicting data protection requirements, creating uncertainty for parties and tribunals regarding the lawful basis for processing personal data. This regulatory inconsistency underscores the need to map and analyse how different legal systems define the legitimacy of data processing and to identify which basis aligns most effectively with the transnational and procedural nature of international arbitration.

This study aims to examine the lawful basis for personal data processing in the context of international arbitration and to assess which of these bases are most suitable for ensuring both procedural efficiency and compliance with global data protection standards. The central research issue arises from the growing tension between the transnational nature of arbitration and the fragmented landscape of data protection laws that define legality in divergent ways. Specifically, the article seeks to identify the points of convergence and divergence among major data protection frameworks, focusing on how consent, contractual necessity, legal obligation, and legitimate interest are interpreted and applied.

This study adopts a comparative legal methodology examining fifteen data protection statutes selected to capture the diversity of global regulatory models and their relevance to international arbitration. The jurisdictions include the European Union, the United Kingdom, Switzerland, China, India, Singapore, Japan, South Korea, Brazil, South Africa, the United Arab Emirates, Australia, Russia, Canada, and the United States (California). These were chosen for three main reasons. First, they represent the principal regulatory philosophies in data protection, including rights-based (e.g., EU, Switzerland and Canada), state-controlled (e.g., China, Russia), hybrid or pragmatic (e.g., India, Brazil, Singapore, UAE), and sectoral (e.g., United States) approaches. Second, they encompass key arbitration jurisdictions and data transfer hubs, ensuring the findings are practically relevant to transnational proceedings. Third, they collectively illustrate the patterns of convergence and divergence in defining lawful bases for processing personal data, ranging from consent and contractual necessity to legitimate interest and public obligation. This broad selection allows the study to identify which legal bases are most adaptable to the cross-border, multi-jurisdictional context of international arbitration.

The article proceeds as follows. Section 2 outlines the conceptual

foundations of lawful basis for processing, situating these principles within the procedural realities of international arbitration. Section 3 presents a comparative mapping of major data protection statutes, identifying the lawful basis most relevant to arbitration and summarising them in a structured table. Section 4 offers an analytical discussion of the patterns and divergences revealed by the comparative analysis. It evaluates which basis is most adaptable to arbitration's transnational framework. Section 5 concludes the article by considering the broader implications of these findings for global data governance and suggests possible avenues for harmonisation or soft-law guidance.

2. CONCEPTUAL FOUNDATIONS OF LAWFUL BASIS FOR DATA PROCESSING

The first principle of data protection laws is that personal data must be processed lawfully and fairly. This was first established by the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines) and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). OECD Guidelines state that data should be acquired through lawful and equitable means with the knowledge or consent of the data subject.[14] The Convention 108 echoes a similar principle, focusing solely on the concept of 'lawful collection'.[15] The principle was subsequently incorporated into Article 6 of Directive 95/46/EC and Article 5 (1) (a) of the GDPR.[16] Article 5(1)(a) states that personal data should be 'processed lawfully, fairly, and in a transparent manner in relation to the data subject.'[17]

The GDPR stipulates that personal data processing is deemed lawful if it satisfies at least one of the following conditions: clear consent from the data subject for specific purposes, necessity for contract performance or pre-contractual steps, compliance with legal obligations, protection of vital interests of the data subject or

[14] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (adopted by the Council of the OECD, 23 September 1980, as amended 11 July 2013) para 7.
[15] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, CETS No 108 (Convention 108) art 5(a) <http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm> accessed 22 September 2025.
[16] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31, art 6.
[17] GDPR (n 6) art 5 (1)(a).

other persons, execution of public tasks or official authority, or pursuit of legitimate interests of the controller or any third party.[18] However, the Convention 108 and OECD Guidelines did not provide such an explicit list. This comprehensive enumeration of lawful reasons for data processing is a significant accomplishment of EU data regulations.

Article 9 of the GDPR categorises certain personal data as special and establishes a strict prohibition on processing 'special categories' of personal data.

> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.[19]

Article 9(2) nevertheless provides exceptions permitting such processing for specific circumstances, such as explicit consent, necessity for the establishment, exercise or defence of legal claims, substantial public interest, or for reasons of vital interest.[20]

Article 13 of the PIPL similarly requires a lawful basis, listing consent as primary but also allowing processing for contractual necessity, statutory duties, public health emergencies, public interest reporting, and other circumstances provided by law.[21] By contrast, the DPDPA takes a narrower approach, it recognises consent and certain legitimate uses defined in section 7,[22] such as for compliance with legal obligations to 'disclose any information to the State or any of its instrumentalities',[23] 'for compliance with any judgment or decree or order',[24] state functions, medical emergencies or employment-related purposes.[25] Thus, while the GDPR offers the most plural and balanced set of lawful bases, the PIPL leans heavily on consent but incorporates state and public interest grounds, whereas the DPDPA adopts a simpler dual model of consent plus limited state-defined legitimate uses, giving the government wide discretion.

[18] Ibid art 6(1).
[19] GDPR (n 6) art 9 (1).
[20] Ibid art 9(2).
[21] PIPL (n 10) art 13.
[22] DPDPA (n 9) art 4.
[23] Ibid art 7 (d).
[24] Ibid art 7(e).
[25] Ibid art 7.

On the other hand, Switzerland's Federal Act on Data Protection (FADP, 2023) adopts a principle-based approach rather than an enumerative one to the lawful processing of personal data. Unlike the GDPR, which lists six distinct legal bases in Article 6(1), the FADP does not require private controllers to identify a specific statutory ground before processing. Instead, it assumes that processing is lawful so long as it complies with core data protection principles, such as proportionality, purpose limitation, transparency, and good faith, and does not contravene the express wishes of the data subject.[26] A separate legal justification becomes necessary only when these principles are violated, when sensitive data is disclosed to third parties, or when processing is contrary to the individual's express refusal. In such cases, Article 31(1) requires justification through consent, an overriding private or public interest, or a legal obligation.[27] Federal bodies, by contrast, must always rely on a statutory basis, reflecting the higher accountability expected of public authorities.[28]

A similar structure can be observed in Japan's Act on the Protection of Personal Information (APPI) and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), which also rely on broad notions of 'appropriate purposes' or 'reasonable expectations' rather than fixed legal bases.[29] These systems emphasise the contextual legitimacy of data processing over formalistic enumeration, aligning lawful processing with the overall fairness of conduct. However, this flexibility can also create uncertainty in transnational contexts, such as international arbitration, where GDPR-based systems require explicit legal grounds, while FADP or APPI-style systems rely on implicit justification through overriding interests. Consequently, although Switzerland's FADP achieves functional compatibility with the GDPR in practice, it represents a distinct conceptual model, one that entrusts lawful processing to principled judgment rather than procedural categorisation.

2.1 Grounds for Lawful Processing

In practical scenarios, data controllers or processors must provide evidence that at least one of the specified legal grounds justifies their processing of personal data.[30] Notably, there is no hierarchical ranking among the grounds for lawful processing;

[26] Federal Act on Data Protection (Switzerland) (FADP) of 25 September 2020 (entered into force 1 September 2023) arts 6 and 30.
[27] Ibid art 31(1)–(2).
[28] Ibid art 34.
[29] Act on the Protection of Personal Information (Japan) (Act No 57 of 2003, as amended 2020, effective 2022) arts 16–23; Personal Information Protection and Electronic Documents Act (Canada) SC 2000, c 5, Principle 4.3, s 5(3).
[30] GDPR (n 6) art 6(1).

none holds normative priority over the others.[31] In the context of international arbitration, several lawful grounds under GDPR Article 6(1) are directly relevant, including clear consent of participants, processing necessary for the performance of a contract or pre-contractual steps, compliance with legal obligations, and the pursuit of legitimate interests of the controller or a third party. The PIPL, however, does not recognise 'legitimate interests' as an independent basis for processing, thereby narrowing the options and making consent, contractual necessity, or statutory duties the primary grounds available in arbitration settings.[32] By contrast, the DPDPA adopts an even more limited approach, for arbitral proceedings processing can be justified only on the basis of consent or compliance with a judgment, decree, or order.[33]

2.1.1 *Processing with Clear Consent*

Article 8(2) of the CFREU states that personal data 'must be processed [...] on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.[34] The GDPR defines 'consent' as:

> '[...] any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[35]

According to this definition, consent must meet four key conditions, i.e., it must be freely given (without coercion or imbalance of power), specific (tied to a particular purpose of processing), informed (the individual understands what data will be processed, by whom, and for what reason), and unambiguous (expressed through a clear statement or affirmative action, not silence or pre-ticked boxes).[36] In other words, valid consent requires an active choice by the data subject, demonstrating real control over their personal data.

Under the GDPR, the criterion 'freely given' requires that

[31] Waltraut Kotschy, 'Article 6 Lawfulness of processing' In Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 321, 329.
[32] PIPL (n 10) art 13.
[33] DPDPA (n 9) art 7.
[34] Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 8(2).
[35] GDPR (n 6) art 4(11).
[36] Lee A Bygrave and Luca Tosoni, 'Article 4(11). Consent' in Christopher Kuner and others (eds) (n 31), 174, 181.

the data subject has substantial autonomy in their decision to consent. As per the Article 29 Working Party (WP29)'s guidance, consent is not deemed valid if the data subject feels they have no genuine choice, is pressured into consenting, or face adverse consequences for not consenting. Furthermore, if withdrawing consent harms the data subject, this also fails to meet the necessary standard.[37] The criteria for 'specific' consent necessitate a direct connection between the consent given and the particular data processing activity. This involves the data controller clearly outlining the scope of the processing activity for which the data subject's consent is sought and effectively communicating this scope to the data subject. The WP29 emphasises that consent must be tied to a specific purpose, and a purpose that is too broad or ill-defined will typically fail to satisfy the condition of being 'specific'.[38] This specific communication with comprehensive details about the nature of the data processing activity to which they are being asked to consent is crucial.[39] Therefore, the requirements of specificity and informed consent are closely intertwined.

The final criterion of consent must be 'non-ambiguous'. Recital 32 of the GDPR expands on this requirement, stating that consent must be unmistakable and expressed through a definitive affirmative action that leaves no doubt as to the data subject's consent. This could be in the form of a written or oral statement or any other clear action. The recital emphasises that consent cannot be inferred from non-actions, such as silence, default options, or a lack of response.

The GDPR imposes the most stringent requirements for valid consent. Under Article 7(1) of GDPR, data controllers must demonstrate that consent was obtained legitimately for a particular data processing activity. Therefore, they bore the burden of proving specific consent and must employ dependable methods to secure such consent, with due consideration for the sensitivity of the data processing operation in question.[40] Article 7(2) states that any request for consent must be prominently distinct when included within a broader written statement. This ensures that the

[37] Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259 rev.01, adopted 28 November 2017, revised 10 April 2018) 5 and 7.
[38] Article 29 Data Protection Working Party (n 37) 12.
[39] Ibid 13.
[40] Eleni Kosta, 'Article 7 Conditions for consent' in Christopher Kuner and others (eds) (n 31) 345, 349.

consent request is presented in a simple language that is easy to understand and access.

Article 7(3) of the GDPR states that data subjects can revoke consent at any time, and data controllers must inform them of this right beforehand. The process to withdraw consent should be as simple as giving it. However, withdrawing consent does not retroactively illegitimise past data processing. If other legal grounds exist for processing, it may continue even after consent is withdrawn, provided that data subjects are informed of the new basis for processing.[41] Article 7(4) of the GDPR requires that consent should be freely given and aims to limit the practice of requiring consent for 'bundling' or 'tying' data processing as a condition for accessing services or goods as a part of a contract.[42] It does not completely ban such practices but creates a presumption against freely given consent when bundling occurs.[43]

The GDPR also requires explicit consent in situations involving heightened risks, such as processing special categories of personal data,[44] data transfers without adequate safeguards,[45] and the use of automated decision-making or profiling.[46] Unlike 'regular' consent, which already requires a clear affirmative action, explicit consent demands an express statement from the data subject, ensuring a higher degree of clarity and proof.[47] While a written and signed declaration is the most secure method, explicit consent can also be provided through electronic means, such as completing an online form, sending an email, uploading a signed document, or using an electronic signature.[48] Even oral consent may be valid if sufficiently recorded, though it poses greater evidentiary challenges.[49] In essence, explicit consent under the GDPR ensures unequivocal expression and verifiability of the individual's agreement.

The GDPR sets the most detailed and uniform standard, i.e., consent must be freely given, specific, informed, and

[41] Ibid 351.
[42] Eleni Kosta (n 40) 352.
[43] Case C-673/17 *Planet49 GmbH* [2019] ECLI:EU:C:2019:246, Opinion of AG Szpunar, para 98.
[44] GDPR (n 6) art 9.
[45] Ibid art 49.
[46] Ibid art 22.
[47] Article 29 Data Protection Working Party (n 37) 18.
[48] Article 29 Data Protection Working Party (n 37) 18.
[49] Ibid.

unambiguous, demonstrated through clear affirmative action, and revocable at any time. The PIPL also requires voluntary, explicit, and informed consent but goes further by demanding separate consent for sensitive data, third-party sharing, public disclosure, and cross-border transfers.[50] The DPDPA, meanwhile, follows the GDPR's core conditions of free, specific, and unambiguous consent,[51] but distinguishes itself by creating the Consent Manager mechanism, which allows independent entities to manage and withdraw consent in an accessible and interoperable way.[52] In practice, the GDPR provides the strictest legal framework, the PIPL heightens substantive safeguards for high-risk processing, and the DPDPA strengthens procedural control through institutional oversight.

2.1.2 *Processing for Contractual Performance*

The GDPR also provides a legal basis for data controllers to process personal data when 'processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.'[53] The PIPL also provides similar provisions in article 13(ii). The European Data Protection Board (EDPB) suggested that determining what is necessary for contract performance requires an objective analysis before processing begins. This includes evaluating all facts and considering alternative, less intrusive methods to fulfil the contract.[54] If no alternatives are available to process the specific personal data, the controller must show that processing was conducted to fulfil the contract's fundamental purposes.[55] Unlike situations where consent is the basis for data processing, a data subject who is a party to a contract cannot unilaterally stop the processing except if the contract itself is

[50] PIPL (n 10) art 14.
[51] DPDPA (n 9) s 6.
[52] ' "Consent Manager" means a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.' DPDPA (n 9) art 2(g).
[53] GDPR (n 6) art 6(1)(b).
[54] EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, Version 2.0 (8 October 2019) 8 <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf> accessed 27 September 2025.
[55]EDPB (53).

terminated.

Article 6(1)(b) of the GDPR also covers processing personal data in pre-contractual scenarios, such as creating a proposal for a travel package. Lawful data processing in pre-contractual contexts under Article 6(1)(b) should be confined strictly to the 'necessary' actions, as commonly understood and practised, to meet the data subject's request.[56] Processing is lawful only within the bounds of what the data subject would reasonably expect and what is customarily sufficient for the type of request the data subject makes.[57]

2.1.3 *Processing for Legal Obligation*

Article 6(1)(c) of the GDPR provides a lawful ground for processing personal data when processing is required to comply with legal obligations under EU or Member State law. The wording of Article 6(1)(c) of the GDPR is not specific about the kinds of legal obligations it encompasses. Traditionally, it has been interpreted to apply only to obligations directly imposed by legal statutes and secondary legal acts, like delegated legislation or a specific binding decision made by a public authority, rather than those arising from agreements between private individuals or entities.[58] It excludes obligations under third-country laws unless integrated into EU law, member state law, and international agreements.[59]

Article 13(3) of China's PIPL also establishes a similar ground by allowing processing when necessary to perform statutory duties or legal obligations, but the scope extends to both private and public entities.[60] Meanwhile, the Indian DPDPA narrows the legal obligation ground significantly, permitting processing only where disclosure of personal data is mandated by Indian law to the State or its instrumentalities.[61] This creates a more restrictive framework, limiting the legal obligation ground primarily to state-facing compliance, unlike the GDPR's broader

[56] Ibid 13.
[57] Ibid.
[58] Article 29 Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (WP 217, 9 April 2014) 19 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> accessed 27 September 2025.
[59] Waltraut Kotschy (n 31) 333.
[60] PIPL (n 10) art 13(III).
[61] DPDPA (n 9) art 7(d).

application to both private and public obligations.

2.1.4 *Legitimate Interests*

Article 6(1)(f) of the GDPR allows data processing based on the legitimate interests of the controller or a third party. GDPR ensures that legitimate interests must be lawful, often grounded in EU or Member State law, and cannot be justified solely by commercial interests.[62] They should align with the fundamental rights and freedoms acknowledged by the Charter of Fundamental Rights of the European Union, as these rights can be sources of legitimate interests.

Under Article 6(1)(f) of the GDPR, data processing based on legitimate interests is not permissible if it is outweighed by the interests or fundamental rights and freedoms of the data subject necessitating personal data protection.[63] Controllers must conduct a 'balancing test' aligned with proportionality principles. The WP29 provided guidelines for this test under Article 7(f) of the Data Protection Directive, which remain relevant for GDPR Article 6(1)(f). The test includes: (a) evaluating the controller's legitimate interest, (b) considering the impact on data subjects, (c) establishing a provisional balance, and (d) implementing safeguards to mitigate any adverse effects on data subjects.[64] This assessment is crucial for accountability and must be completed and documented before initiating processing activities to ensure compliance with the controller's duties.

3. COMPARATIVE MAPPING OF LAWFUL BASES

Table 1: Lawful Bases for Processing Personal Data[65]

Jurisdiction	Principal law	Main lawful bases	Remarks on applicability to international arbitration

[62] Waltraut Kotschy (n 31) 337.
[63] Ibid 338.
[64] Article 29 Working Party (n 58) 29–30.
[65] Table 1, compiled by the author from primary statutes and official regulatory materials (see Source note in every row).

European Union	GDPR Art. 6(1)(a)–(f)	Consent; Contract; Legal obligation; Vital interests; Public task; Legitimate interests	Legitimate interest and contractual necessity are commonly used to justify procedural processing (evidence exchange, case management) without repeated consent.[66]
United Kingdom	UK-GDPR (Data Protection Act 2018)	Same six bases as GDPR (Art 6)	Same practical approach as the EU; London is a major seat, a legitimate interest, and a contract widely relied on.[67]
Switzerland	Federal Act on Data Protection (FADP, 2020/2023), Art 6, 30, 31	Principle-based: processing lawful unless it breaches personality rights; where needed: consent; overriding private/public interest; law	Private controllers generally need no formal 'legal ground' unless principles or the subject's wishes/sensitive data are implicated; arbitration institutions have practical flexibility but must show proportionality.[68]
China	PIPL (2021), Art 13	Closed list: Consent; Necessary for contract; Necessary for statutory duties/obligations; emergencies; public interest; lawfully	No 'legitimate interest' ground, contract basis limited to contracting parties; statutory duty limited to legal/statutory obligations (not procedural arbitration needs). This makes non-consensual processing in arbitration more constrained.[69]

[66] GDPR (n 6) art 6(1).
[67] Information Commissioner's Office (ICO), 'A guide to lawful basis' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/> accessed 11 September 2025.
[68] FADP (n 26) arts 6, 30–31.
[69] PIPL (n 10) art 13.

		disclosed info; other laws	
India	Digital Personal Data Protection Act (DPDPA), 2023, ss.6–7	Consent; enumerated 'legitimate uses'(e.g., employment, compliance with judgments/orders, state functions, etc.	No open 'legitimate interest'; arbitration processing must normally be based on consent or 'deemed consent' (e.g., where service is requested)[70]
Singapore	PDPA (Personal Data Protection Act) 2012 (Amendment Act 2020), ss.13–17	Consent as default; exceptions added by amendment: legitimate interests/business improvement exceptions (post-2020)	Since 2020, the PDPA has included exceptions akin to legitimate interest/business exceptions, which are workable for arbitration, including institutional processing and administrative uses where consent is impractical.[71]
Japan	APPI (Act on the Protection of Personal Information), Arts 18–23 (amended 2020/2022)	Consent default; exceptions include legal obligation; protection of rights/interests; and use within original stated purpose (Art.18(3))	APPI is consent-first, but Art. 23(1)(iii) (protection of rights/interests) functions as a limited analogue to legitimate interest, allowing processing for legal claims/defence; thus APPI is relatively arbitration-compatible.[72]

[70] DPDPA(n 9) arts 6–7.
[71] Personal Data Protection Act 2012 (Singapore) (2020 Rev Ed, Cap 26) ss 13–17.
[72] Act on the Protection of Personal Information (Japan) (Act No 57 of 2003, as amended 2020, effective 2022) arts 18–23.

South Korea	PIPA (Personal Information Protection Act), Art. 15(1) (amended 2023)	Consent; Legal obligation; Contractual necessity; Public duties; Legitimate interests; other special cases	Explicit legitimate interests ground (with balancing test), closely aligned with GDPR; covers processing necessary for litigation/arbitration and institutional functions.[73]
Brazil	LGPD (Law No.13,709/2018), Art 7(I–X)	Consent; Contract; Legal obligation; Public policy; Research; Judicial, administrative or arbitral proceedings; Legitimate interests	LGPD expressly mentions arbitral proceedings, one of the clearest statutory anchors for arbitration-related processing.[74]
South Africa	POPIA (Protection of Personal Information Act), s.11(1)	Consent; Contract; Legal obligation; Public law duty; Legitimate interest	POPIA mirrors an EU-style multi-ground approach, with legitimate interest and contractual necessity available for arbitration scenarios.[75]
United Arab Emirates	Federal Decree-Law No. 45 of 2021	Consent; Contract; Legal obligation; Vital/public interest; Legitimate interest (text and	GDPR-inspired; legitimate-interest and contract grounds usable for arbitration; be mindful of free-zone regimes (DIFC/ADGM have their own rules).[76]

[73] Personal Information Protection Act (South Korea) (Act No 19280, amended 2023) art 15(1).
[74] Lei n° 13.709, de 14 de agosto de 2018 (Lei Geral de Protec¸a˜o de Dados Pessoais) (Brasil) art 7(I–X).
[75] Protection of Personal Information Act 4 of 2013 (South Africa) s 11(1).
[76] Federal Decree-Law No 45 of 2021 Regarding the Protection of Personal Data (UAE).

		exceptions)	
Australia	Privacy Act 1988 (Cth), Australian Privacy Principles (APPs), esp. APP 6	Consent (implicit/explicit); APPs contain lawful purposes and exceptions (including use for legal claims/administration)	Consent default, but APP framework and specific legal exceptions (used to establish, exercise or defend legal claims) make arbitration-related processing (administration, enforcement) permissible under appropriate APP exceptions.[77]
Russia	Federal Law No.152-FZ on Personal Data (2006, amended), Art 6(1)	Consent; legal obligation; participation in court or arbitration proceedings (Art 6 (1)(3)); enforcement of judicial acts (Art 6 (1)(3.1)); contract; legitimate interests of controller or third parties (Art 6 (1)(7)); etc.	Explicitly recognises arbitration proceedings as a lawful basis and includes a legitimate-interest ground, providing strong legal support for arbitral data processing.[78]
Canada	PIPEDA (Personal Information Protection and Electronic Documents Act)	Consent default; Exceptions: 'reasonable purposes' / business purposes; s.5(3) (reasonable purposes test)	PIPEDA's 'reasonable purposes' test functions similarly to a legitimate-interest balancing test; contractual necessity and legal obligations are also applicable. PIPEDA is relatively arbitration-friendly.[79]

[77] Privacy Act 1988 (Cth) sch 1, s 16A, Australian Privacy Principle 6.
[78] Federal Law No 152-FZ on Personal Data (Russian Federation) (2006, as amended) art 6.
[79] Personal Information Protection and Electronic Documents Act (Canada) (PIPEDA) SC 2000, c 5.

United States (California)	CCPA / CPRA Cal. Civ. Code §§1798.100 et seq. (state framework)	No single federal lawful-basis model; California law focuses on consumer rights, opt-outs, and business purposes; contractual necessity and legal obligations recognised in practice	The U.S. is fragmented; many arbitration uses are covered by business purposes or contractual necessities, or sectoral federal laws (e.g., FINRA, HIPAA) — practitioners must combine federal, state, and sectoral rules for compliance.[80]

Table 1 reveals a noticeable pattern of convergence and divergence in how jurisdictions legally enable the processing of personal data relevant to international arbitration. Most jurisdictions, whether influenced directly by the GDPR or shaped by domestic developments, accept consent, contractual necessity, and legal obligations as foundational grounds for data processing. This reflects an increasing harmonisation of principles across legal systems. Jurisdictions such as the EU, UK, South Korea, South Africa, Brazil, and UAE exemplify this convergence, having adopted a multi-ground framework that balances individual autonomy (through consent) and operational necessity (through contract and legitimate interests). The fact that several non-EU jurisdictions, particularly Brazil, South Africa, the UAE and South Korea (PIPA), explicitly recognise 'legitimate interests' shows how GDPR's normative influence has extended globally, establishing a baseline model for data protection governance that can adapt to diverse legal traditions.

Despite general convergence, Table 1 also reveals sharp variations in legal philosophy and operational flexibility. Jurisdictions such as China (PIPL) and India (DPDPA) adopt a state-centric closed-list approach, limiting lawful bases to enumerated statutory categories and deliberately omitting a broad 'legitimate interest' provision. This creates a more consent-centric and state-controlled data protection framework, prioritising individual protection and state oversight over private-sector flexibility. Similarly, Switzerland's FADP stands apart conceptually. It presumes processing is lawful unless personality rights are

[80] California Civil Code (CCPA/CPRA) § 1798.100 et seq.

infringed, at which point justification must derive from consent, overriding interests, or law.[81] This approach diverges from the exhaustive-list model of the GDPR by embedding lawfulness in the principles of proportionality and harm, rather than relying on prescriptive legal bases. Meanwhile, common-law jurisdictions, such as Australia and Canada, adopt more pragmatic, purpose-based tests, 'reasonable purpose' or 'establish, exercise or defend legal claims', allowing for broader discretion but also introducing interpretive uncertainty.[82]

4. IMPLICATION IN INTERNATIONAL ARBITRATION

From the perspective of international arbitration, the legal diversity reflected in Table 1 carries significant operational and compliance implications. Arbitration commonly requires the cross-border transfer and processing of personal data, for instance, handling evidence, witness statements, and tribunal communications, making the availability of non-consensual lawful bases critical. Jurisdictions with legitimate interest or explicit legal-claim exceptions (such as the EU, UK, Brazil, South Korea, and Japan) provide the most practical alignment with arbitral procedures, as these grounds justify processing necessary for the 'establishment, exercise or defence of legal claims.' In contrast, countries without such bases, namely China and India, rely on consent or narrow statutory obligations, which complicates multi-party proceedings and institutional data management. Brazil's LGPD notably stands out by explicitly including arbitral proceedings as a lawful ground, setting a clear model.[83]

4.1 The Limitations of Consent, Contractual Necessity, and Legal Obligation

The legal basis of prior consent of data subjects is often considered appropriate and easy to implement. However, Emily Hay argued that consent is problematic in the context of arbitration.[84] The GDPR defines consent as 'freely given, specific, informed, and unambiguous.'[85] The EDPB has interpreted valid consent as being as easy to withdraw as it is to give, and it cannot be implied.[86] In international arbitration, obtaining consent from

[81] FADP (n 26) arts 6.
[82] PIPEDA (n 79) s 5(3); Privacy Act 1988 (n 77) APP 6.2 (c).
[83] LGPD (n 74) art 7 VI.
[84] Emily Hay, 'Chapter 7: Data protection and international arbitration: never the twain shall meet?' in Pietro Ortolani , André Janssen , et al. (eds), *International Arbitration and Technology* (Wolters Kluwer 2022) 101, 113.
[85] Ibid.
[86] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' (4 May 2020) 7 <https://edpb.europa.eu/our-work-tools/our-

all individuals mentioned in arbitral documents and evidence, particularly those not directly involved or affiliated with the opposing party, is impractical. Additionally, finding an alternative legal basis for processing is difficult once consent is withdrawn. It will potentially disrupt proceedings.

EDPB commented that consent, though initially appealing, is complex and cumbersome.[87] While it is not the most suitable basis for processing personal data in arbitral proceedings under the GDPR, other jurisdictions may also require its use. In cases where an arbitral participant is subject to both the GDPR and the consent requirements of another jurisdiction, compliance becomes challenging due to the absence of a universally accepted conflict of law rule.[88] In such situations, controllers must weigh the separate obligations of each law and determine the most appropriate solution. The chosen solution must be transparent to data subjects, possibly through a privacy notice, regarding the basis for processing their data.

Similarly, contractual necessity under Article 6(1)(b) GDPR or its equivalents only justifies processing for data subjects who are parties to the contract, that is, the arbitration agreement itself.[89] It does not extend to third parties whose data may appear in evidence, correspondence, or submissions. Another legal basis, 'compliance with a legal obligation', is a potential ground for processing personal data. The GDPR specifies that such processing must be based on EU or Member State law. WP29 noted that obligations arising from foreign statutes or EU regulations may not qualify unless they are incorporated into Member State law.[90] Arbitration is, by design, a private mechanism rather than a state-mandated procedure; therefore, data processing during arbitral proceedings typically does not arise from obligations imposed by law, except in narrow regulatory contexts (e.g., anti-money-laundering compliance). Consequently, these three grounds collectively fail to provide a consistent or comprehensive lawful basis for the routine data exchanges integral to arbitration.

4.2 The Functional Advantage of Legitimate Interests

Figure 1: Appropriate Lawful Bases for Data Processing in

documents/guidelines/guidelines052020-consent-under-regul> accessed 22 May 2024.

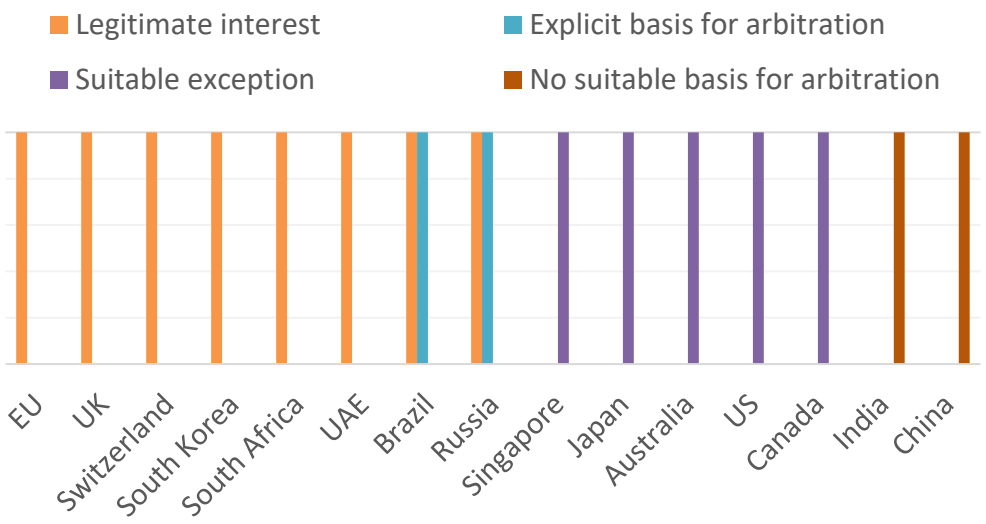
[87] Ibid.

[88] Emily Hay (n 84) 114.

[89] GDPR (n 6) art 6(1)(b).

[90] Article 29 Data Protection Working Party, 'Working Document 1/2009 on Pre-trial Discovery for Cross Border Civil Litigation' (00339/09/EN WP 158, 2009) 9.

International Arbitration[91]



As illustrated in Figure 1, most jurisdictions recognise legitimate interests directly or indirectly, reinforcing its status as the de facto global standard for non-consensual lawful processing. The exceptions, China and India, reveal distinct regulatory philosophies. China's PIPL adopts a closed-list approach, excluding legitimate interests and emphasising consent, contract, or statutory duties, thereby constraining the flexibility of private entities.[92] India's DPDPA follows a similar model, recognising limited 'legitimate uses' but not a general balancing test akin to legitimate interest. Section 7(e) permits processing to comply with judgments or orders, but this applies only after adjudication, not to ongoing arbitral proceedings.[93]

The absence of a legitimate-interest provision in these jurisdictions complicates data handling in arbitrations involving parties or evidence connected to them. Arbitral institutions and practitioners must either rely on narrow consent or conduct jurisdiction-specific compliance exercises to ensure data protection compliance. Conversely, jurisdictions that adopt a legitimate interest approach allow for more coherent and pragmatic data governance during arbitration. EU regulators acknowledge its relevance in cross-border discovery in US legal proceedings, where justice is served by not unduly restricting an

[91] Figure 1, compiled by the author, based on data protection statutes listed in Table 1. This figure illustrates the presence or absence of a legitimate interest or equivalent lawful ground for personal data processing across fifteen jurisdictions surveyed.
[92] PIPL (n 10) art 13.
[93] DPDPA (n 9) art 7(e).

organisation's ability to promote or defend legal rights.[94] Similarly, making or defending a legal claim in arbitration or administering dispute resolution is considered a legitimate interest under the GDPR. Unlike national courts, arbitration lacks the legal basis for the necessary processing to perform a task in the public interest or exercise official authority vested in the controller.

In arbitration, the more pertinent the data to resolving a dispute, the stronger the legitimate interest in processing it. However, Legitimate interests cannot be treated as an unrestricted legal basis for data processing in arbitration.[95] An interest qualifies as 'legitimate' under Article 6(1)(f) only when several cumulative conditions are met. First, the interest must be lawful, meaning it cannot contravene EU or Member State law, even though it need not be explicitly recognised by statute.[96] Second, the interest must be clearly and specifically defined so that its scope can be properly weighed against the data subject's rights and freedoms.[97] Third, it must be real and current, not speculative or hypothetical at the time of processing.[98]

This balancing exercise may justify one type of processing, such as filing a witness statement that is essential for establishing a claim or defence, while restricting another, such as publishing the same statement in unredacted form where it contains sensitive or unnecessary personal details. In practice, tribunals and parties may need to rely on redaction as a safeguard when arbitral evidence contains third-party data, sensitive health information, or other details that are irrelevant to the dispute. Excluding an entire document from the record is rare and typically occurs only when the document is wholly irrelevant or when redaction would not adequately protect privacy interests.

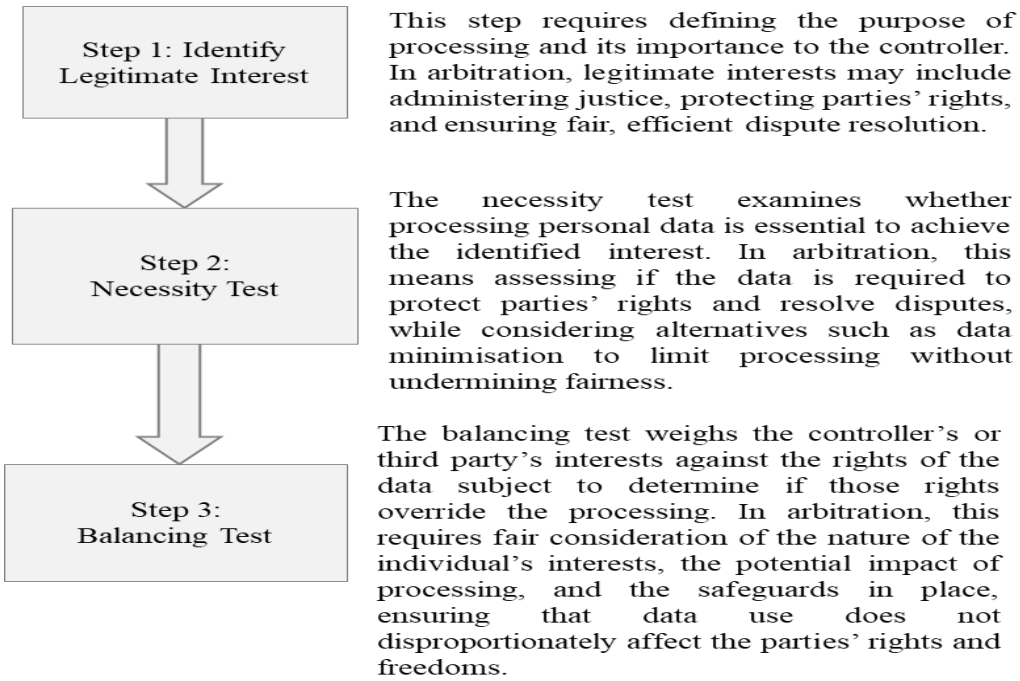
However, to rely on legitimate interest, GDPR requires arbitral participants to apply the structured three-step test set out in the EDPB Guidelines 1/2024 (see Figure 2).[99] This begins with the clear identification of a legitimate interest, such as preparing and presenting evidence, ensuring procedural transparency, or

[94] European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), 'ANNEX: Preliminary comments on the US CLOUD Act' (Joint Response, 10 July 2019) 5.
[95] EDPB, 'Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR' (Version 1.0, 8 October 2024) paras 12–13 <https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf> accessed 11 September 2025.
[96] Ibid para 17.
[97] EDPB (n 95) para 17.
[98] Ibid.
[99] EDPB (n 95) paras 14, 28 & 31.

protecting the integrity of the proceedings.[100] Moreover, the existence of such an interest is not in itself sufficient. The controller must also demonstrate that processing the personal data is strictly necessary to achieve the identified purpose and that the objective cannot reasonably be attained through less intrusive means, such as redaction, pseudonymisation, or limiting disclosure.[101] Finally, a balancing exercise must be conducted to ensure that the rights and freedoms of the data subject do not override the interest pursued.[102] In arbitration, this balancing often requires particular care where sensitive or third-party data is involved, since disclosure can have significant reputational and legal consequences.

To ensure consistency with the accountability principle under Article 5(2) GDPR, arbitral participants should also document the assessment and, where applicable, involve a Data Protection Officer to ensure compliance.[103] By following the EDPB's structured approach, arbitration participants can demonstrate that reliance on legitimate interest as a legal basis respects both the efficiency of the arbitral process and the fundamental rights of data subjects.

Figure 2: Three-Part Test for Legitimate Interests Assessment[104]



[100] Ibid paras 14–18.
[101] Ibid paras 28–30.
[102] Ibid paras 31–34.
[103] GDPR (n 6) art 5(2) and 36.
[104] Figure 2, compiled by the author, based on EDPB Guidelines 1/2024 (n 95).

5. CONCLUSION

The comparative analysis of major data protection regimes reveals that, despite their diverse legislative frameworks and underlying philosophies, a harmonisation is evident. The recognition of legitimate interests, whether explicitly or implicitly, provides a flexible legal basis for arbitral processing of personal data. In international arbitration, vast quantities of personal data are exchanged and processed across borders for the purposes of case preparation, evidence production, and adjudication. Traditional lawful bases such as consent, contractual necessity, and legal obligation prove inadequate in this setting. Consent is impractical due to the multiplicity of data subjects and the imbalance of procedural control. Contractual necessity is limited to the parties' own data and does not extend to third-party information embedded in arbitral materials. Legal obligation seldom applies, as arbitration is a private dispute resolution mechanism rather than a statutory function.

Among the fifteen jurisdictions examined, thirteen recognise legitimate interests or equivalent exceptions that can accommodate the data processing inherent in arbitration. Only China and India deviate from this trend, reflecting state-centric or consent-based models that prioritise individual control over pragmatic flexibility. This divergence underscores the persistence of normative pluralism in global data protection law, which complicates cross-border arbitral practice. Nevertheless, the widespread recognition of legitimate interest provides a conceptual bridge for reconciling data protection compliance with arbitral efficiency and confidentiality.

Notably, Brazil's LGPD and Russia's Federal Law No.152-FZ directly recognise arbitration as a legitimate ground for data processing, setting an important precedent for other jurisdictions. Similarly, Switzerland's Federal Act on Data Protection (FADP) adopts a more principle-based model, allowing processing so long as it adheres to fundamental data protection principles or is not contrary to the data subject's express wishes. These models illustrate alternative approaches that accommodate the realities of arbitral practice without rigidly enumerating lawful bases. So, this study highlights the need for a more harmonised interpretive framework that explicitly recognises international arbitration as a legitimate and necessary context for data processing.