Т. 12. №3 2026
https://doi.org/10.33619/2414-2948/124

UDC 341.1 https://doi.org/10.33619/2414-2948/124/50

INTERNATIONAL STANDARDS FOR DATA PROTECTION AND CROSS-BORDER FLOWS

*©**Tursunbaeva N.**, ORCID:0000-0002-8336-6264, SPIN code:4664-5594, Ph.D.,*
Kyrgyz-Russian Slavic University, Bishkek, Kyrgyzstan, nazira.tursunbaeva@gmail.com
*©**Abolfazl Arab**, Kyrgyz-Russian Slavic University,*
Bishkek, Kyrgyzstan, abolfazlara1081@gmail.com

МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ЗАЩИТЫ ДАННЫХ И ТРАНСГРАНИЧНЫХ ПОТОКОВ

*©**Турсунбаева Н. С.**, ORCID: 0000-0002-8336-6264, SPIN-код: 4664-5594,*
канд. юрид. наук, Кыргызско-Российский славянский университет,
г. Бишкек, Кыргызстан, nazira.tursunbaeva@gmail.com
*©**Аболфазл Араб,** Кыргызско-Российский славянский университет,*
г. Бишкек, Кыргызстан, abolfazlara1081@gmail.com

Abstract. The rapid expansion of the digital economy and the exponential growth of data transmitted across national borders have made the harmonisation of personal data protection regimes a central issue in contemporary international law. Using comparative legal analysis, this article examines international, regional, and national legal instruments governing cross-border transfers of personal data. These include the Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as modernised, the European Union General Data Protection Regulation and its recent adequacy decision concerning the United States, the Asia-Pacific Economic Cooperation and Global Cross-Border Privacy Rules systems, the Organisation for Economic Co-operation and Development Declaration on Government Access to Personal Data, United States national security regulations adopted under Executive Order No. 14117, China's simplified 2024 rules on cross-border data transfers, Brazil's 2024 regulation on international data transfers, and Russia's 2025 amendments on data localisation. The article evaluates trust-building mechanisms, including standard contractual clauses, binding corporate rules, certification mechanisms, and privacy-enhancing technologies, and assesses the Group of Twenty initiative on Data Free Flow with Trust and related trade policy recommendations aimed at reducing regulatory fragmentation. The study concludes that, in the absence of a universal international treaty, mutual recognition of safeguards and the widespread use of privacy-by-design technologies are essential to balancing the protection of human rights with the promotion of innovation.

Аннотация. Быстрый рост цифровой экономики и экспоненциальное увеличение объёма данных, передаваемых через государственные границы, вывели проблему гармонизации режимов защиты персональной информации в число ключевых вопросов современного международного права. В статье на основе сравнительно-правового анализа рассматриваются международные, региональные и национальные правовые акты, регулирующие трансграничную передачу персональных данных. К ним относятся Руководящие принципы Организации экономического сотрудничества и развития по защите конфиденциальности и трансграничным потокам персональных данных, Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных в обновлённой

Т. 12. №3 2026
https://doi.org/10.33619/2414-2948/124

редакции, Общий регламент Европейского союза по защите данных и новое решение о достаточности защиты данных при передаче в Соединённые Штаты Америки, система правил трансграничной конфиденциальности Азиатско-Тихоокеанского экономического сотрудничества и Глобальная система трансграничных правил, Декларация Организации экономического сотрудничества и развития о доступе государственных органов к персональным данным, нормы национальной безопасности Соединённых Штатов Америки, принятые на основании Исполнительного Указа №14117, упрощённые правила Китайской Народной Республики 2024 года о трансграничной передаче данных, регулирование Бразилии 2024 года и поправки Российской Федерации 2025 года о локализации данных. Анализируются механизмы формирования доверия, включая стандартные договорные условия, обязательные корпоративные правила, сертификационные механизмы и технологии обеспечения конфиденциальности. Делается вывод о том, что при отсутствии универсального международного договора взаимное признание гарантий и внедрение подхода «конфиденциальность по замыслу» являются ключевыми для защиты прав человека и стимулирования инноваций.

Keywords: international standards, personal data protection, cross-border data flows, localisation; trust, law.

Ключевые слова: международные стандарты, защита персональных данных, трансграничные потоки данных, локализация, доверие; право.

Cross-border data transfers underpin everything from cloud computing to artificial intelligence. Despite their economic importance, they raise profound legal and human rights questions. Divergent national approaches to privacy, surveillance and national security have created a fragmented regulatory landscape that imposes compliance costs and threatens to balkanise the digital economy. At the same time, governments, businesses and civil society increasingly recognise the need to share data to tackle global challenges, from pandemics to climate change. This tension between openness and control explains why harmonising international standards for data protection has become a central issue of international law. The purpose of this study is to provide a comprehensive overview of current international frameworks, identify common principles and divergences, and evaluate initiatives that seek to promote trusted data flows. Particular attention is paid to developments in 2024–2025, including new regulations in China, Brazil and Russia, the United States' national security rule on bulk data transfers, the launch of the Global CBPR and Privacy Recognition for Processors (PRP) certifications, and trade policy recommendations to reduce regulatory fragmentation. The novelty of this work lies in synthesising these diverse developments and proposing pathways toward interoperable and human-rights-respecting data governance.

Materials and Methods

This research employs doctrinal analysis, examining legal texts, policy documents and scholarly commentaries. Primary sources include the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the Council of Europe's Convention 108+, the European Union's GDPR and adequacy decisions, the APEC Cross-Border Privacy Rules (CBPR) and the Global CBPR Forum documents, the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, China's 2024 Regulations on Promoting and Regulating Cross-Border Data Flows, Brazil's Resolution CD/ANPD No. 19/2024, Russia's amendments to Federal Law No. 152-FZ effective from July 2025, and the U.S. Department of Justice Final Rule

Т. 12. №3 2026
https://doi.org/10.33619/2414-2948/124

implementing Executive Order 14117. Secondary sources include the World Economic Forum's report on Data Free Flow with Trust (DFFT) and a 2025 trade policy study on navigating cross-border data flows and the GDPR, as well as commentary from legal practitioners. Comparative analysis identifies shared principles (such as purpose limitation, accountability and adequacy) and differences (e.g., localisation versus accountability-based regimes). Developments through 2025 are emphasised to ensure that the analysis reflects the current state of law. Citations are provided in accordance with academic standards [1-11].

Results and Discussion

Global and regional frameworks. OECD Guidelines and Convention 108+. The OECD Guidelines, first adopted in 1980 and revised in 2013, articulate eight principles — collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability — that remain the foundational "soft law" framework for transborder flows [1].

The Council of Europe's Convention 108+, opened for signature in 2018, transforms these principles into binding obligations and is the only international treaty directly addressing cross-border personal data transfers. It requires parties and third countries to provide an adequate level of protection and permits transfers only where such safeguards exist [2].

European Union – GDPR and adequacy decisions. Chapter V of the GDPR regulates international data transfers by establishing three mechanisms: (I) adequacy decisions by the European Commission recognising that a third country or international organisation offers essentially equivalent protection; (II) appropriate safeguards, such as standard contractual clauses (SCCs), binding corporate rules (BCRs) and codes of conduct; and (III) limited derogations for specific situations (https://gdpr-info.eu/).

Recent developments include the EU–U.S. Data Privacy Framework (DPF), adopted in July 2023, which provided a new adequacy decision for the United States after the invalidation of the Privacy Shield. The European Data Protection Board emphasises transparency and accountability in international transfers and continues to develop guidance on new transfer tools. A 2025 Swedish trade study recommends standardising definitions, accelerating adequacy decisions, providing technical assistance to developing economies and creating a "Data Flows Test" for EU policymaking to reduce fragmentation [11].

OECD Declaration on Government Access. In December 2022 the OECD adopted a Declaration on Government Access to Personal Data Held by Private Sector Entities. After two years of negotiation, the declaration identified significant commonalities among democratic states' safeguards for national security and law enforcement access to personal data and became the first intergovernmental agreement on the subject [5].

It aims to increase trust by promoting legal basis, purpose limitation, necessity and proportionality, oversight, transparency and redress. APEC CBPR and the Global CBPR Forum. APEC's voluntary Cross-Border Privacy Rules (CBPR) system emphasises organisational accountability and cooperation. The APEC Privacy Framework's purposes include developing privacy protections, enabling global organisations to implement uniform approaches, assisting enforcement agencies and advancing international mechanisms to promote and enforce information privacy while maintaining continuity of information flows [4].

In May 2022 several economies launched the Global CBPR Forum to expand certification beyond the APEC region. On 2 June 2025 the Forum officially launched the Global CBPR and Privacy Recognition for Processors (PRP) certifications, opening membership to new jurisdictions

Т. 12. №3 2026
https://doi.org/10.33619/2414-2948/124

and announcing a work programme to address sensitive personal information, children's data and breach notification.

Data Free Flow with Trust (DFFT) initiative. The DFFT initiative, proposed by Japan and endorsed by the G20, seeks to develop a framework for free and trusted data flows. The World Economic Forum notes that cross-border data flows underpin the global economy and that national regulations often restrict them, leading to fragmented rules; its white paper maps a multi-dimensional architecture for international cooperation on data flows and highlights the need for trust and interoperability [10].

National frameworks and recent developments. China. China's 2024 Regulations on Promoting and Regulating Cross-Border Data Flows ease compliance burdens by introducing exemptions from standard contractual requirements for transfers involving fewer than 100,000 individuals, necessary transfers for contracts, human resources or emergencies, and by raising thresholds for certification. The regulations aim to facilitate routine cross-border flows while maintaining security assessments and reflect a shift toward an accountability-based approach [6].

Brazil. Brazil's Resolution CD/ANPD No. 19/2024 states that international data transfer must guarantee data protection equivalent to Brazilian law and promotes free cross-border flow while ensuring accountability, transparency and security measures. The resolution defines key terms such as exporter and importer and establishes a framework for contractual clauses and binding corporate rules [7].

Russia. Russia's amendments to Federal Law No. 152-FZ, effective from 1 July 2025, require personal data of Russian citizens to be collected and initially processed using databases located in Russia, effectively localising infrastructure. Cross-border transfers remain possible after initial processing, subject to notification to Roskomnadzor, but additional consent requirements, localisation of cookies and servers and higher fines increase compliance burdens [8].

United States. The U.S. Department of Justice's final rule implementing Executive Order 14117 restricts or prohibits certain "Covered Data Transactions" with "Covered Persons" affiliated with countries of concern (China, Cuba, Iran, North Korea, Russia and Venezuela). It defines thresholds for categories of bulk U.S. sensitive personal data — including genomic data for 100 or more individuals, precise geolocation data for 1,000 or more individuals, personal health data for 10,000 or more individuals and financial information for 100,000 or more individuals — and covers transactions through data brokerage, vendor, employment or investment agreements [9].

Comparative analysis

Despite differences, several common principles emerge across these regimes. Purpose limitation and legal basis: All frameworks require that personal data be collected for specific, legitimate purposes and prohibit secondary use without additional consent or legal justification. Accountability: Controllers must implement measures to ensure compliance, such as data protection impact assessments, security safeguards, contractual clauses, and audits. Adequacy or equivalence: Transfers to third countries generally require evidence that the recipient provides an adequate level of protection. The EU uses binding adequacy decisions; China applies national security assessments or certification; Brazil requires contractual clauses; APEC and the Global CBPR rely on certification; and the U.S. rule prohibits transfers to countries of concern entirely. Individual rights and redress: Most frameworks guarantee rights of access, correction, and redress, though enforcement varies. Transparency and oversight: The OECD Declaration emphasises transparency and independent oversight for government access [5], and national regimes also incorporate supervisory authorities. Localisation versus free flow: Russia mandates data localisation, while China relaxes requirements for routine transfers. Brazil and the EU emphasise accountability rather than localisation. The U.S.

Т. 12. №3 2026
https://doi.org/10.33619/2414-2948/124

rule focuses on national security rather than privacy per se. These differences create compliance burdens and risk fragmentation. Nevertheless, convergence is visible in the adoption of SCCs, BCRs, and certification schemes, and in recognition of privacy-by-design and privacy-enhancing technologies as complements to legal safeguards. The Global CBPR certifications and DFFT roadmap illustrate attempts to build interoperability through mutual recognition rather than imposing a single model.

Trade and policy recommendations. The 2025 Swedish trade study proposes concrete measures to reduce fragmentation while respecting GDPR requirements. Recommendations include developing standardised definitions for key concepts (such as “personal data” and “adequate protection”), accelerating adequacy decisions, providing technical assistance to developing economies, creating a “Data Flows Test” to evaluate the impact of new regulations on data transfers and improving transparency by publishing regulatory proposals and offering multilingual guidance [11].

The study emphasises that strict regulations can impede innovation and that diverse initiatives such as the DFFT and Global CBPR should be considered complementary. It cautions against a world divided into incompatible data governance blocs and urges policymakers to pursue interoperable solutions.

Conclusions

The comparative analysis reveals significant progress toward international convergence in data protection, yet fragmentation persists. The OECD Guidelines and Convention 108+ provide a universal vocabulary but lack enforcement mechanisms. The GDPR remains the most influential model, inspiring reforms in Brazil and driving global debates. However, the absence of a universal treaty allows divergent approaches: accountability-based regimes (APEC/Global CBPR), localisation (Russia), security-driven restrictions (United States) and hybrid models (China). Recent initiatives—such as China’s 2024 regulations easing routine transfers [6], Brazil’s 2024 resolution mandating ANPD-approved contractual clauses [7], Russia’s 2025 localisation amendments [8] and the U.S. DOJ rule prohibiting transfers to countries of concern [9] — illustrate both convergence and new fault lines. The Global CBPR and PRP certifications launched in 2025 offer a promising accountability-based mechanism for interoperability [4]. The OECD Declaration on Government Access demonstrates that democracies can agree on common safeguards [5]. To enable trusted cross-border data flows, policymakers should harmonise transfer mechanisms (e.g., SCCs, BCRs and certifications), promote privacy-by-design and privacy-enhancing technologies, improve transparency and provide technical assistance to developing economies. The DFFT initiative and the G7 roadmap show that pragmatic, bottom-up approaches can address specific barriers. Ultimately, trusted data flows require a shared commitment to digital human rights, innovation and international cooperation.

Источники:

1. Организация экономического сотрудничества и развития. Руководящие принципы по защите неприкосновенности частной жизни и трансграничных потоков персональных данных. Париж: ОЭСР, 2013. 38 с.

2. Совет Европы. Конвенция 108+ о защите физических лиц при автоматической обработке персональных данных. Страсбург: Совет Европы, 2018.

3. Европейский союз. Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года о защите физических лиц в связи с обработкой персональных данных и о свободном обращении таких данных (Общий регламент по защите данных, GDPR).

Т. 12. №3 2026
https://doi.org/10.33619/2414-2948/124

4. Азиатско-Тихоокеанское экономическое сотрудничество (АТЭС). Система трансграничных правил конфиденциальности (CBPR): политика, правила и руководящие принципы. Сингапур: Секретариат АТЭС, 2019.

5. Организация экономического сотрудничества и развития. Декларация об обеспечении государствами доступа к персональным данным, хранящимся в частном. Париж: ОЭСР, 14 дек. 2022.

6. Управление по делам киберпространства КНР. Правила содействия и регулирования трансграничных потоков данных. Пекин: CAC, 22 марта 2024.

7. Национальное управление по защите персональных данных Бразилии (ANPD). Резолюция CD/ANPD №19/2024 о международной передаче персональных данных. Бразилиа: ANPD, 23 авг. 2024.

8. Российская Федерация. Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных» (в ред. Закона №420-ФЗ от 28 нояб. 2024 г.; с изменениями, вступающими в силу 1 июля 2025 г.). Собрание законодательства Российской Федерации. 2006. №31 (ч. I).

9. Министерство юстиции США. Финальное правило: «Предотвращение доступа к конфиденциальным персональным данным США и данным государственного значения странами, вызывающими озабоченность, или соответствующими лицами» (28 CFR, ч. 202). Вашингтон: DOJ, 8 апр. 2025.

10. Всемирный экономический форум. Свободный поток данных с доверием (DFFT): пути к свободным и доверительным потокам данных. Женева: ВЭФ, 2020.

11. Национальный совет по торговле Швеции. Navigating Cross-Border Data Flows and the GDPR: Trade Policy Recommendations. Стокгольм: Национальный совет по торговле Швеции, 2025.

Sources:

1. Organizatsiya ekonomicheskogo sotrudnichestva i razvitiya. Rukovodyashchie printsipy po zashchite neprikosnovennosti chastnoi zhizni i transgranichnykh potokov personal'nykh dannykh. Parizh: OESR, 2013. 38 s.

2. Sovet Evropy. Konventsiya 108+ o zashchite fizicheskikh lits pri avtomaticheskoi obrabotke personal'nykh dannykh. Strasburg: Sovet Evropy, 2018.

3. Evropeiskii soyuz. Reglament (ES) 2016/679 Evropeiskogo parlamenta i Soveta ot 27 aprelya 2016 goda o zashchite fizicheskikh lits v svyazi s obrabotkoi personal'nykh dannykh i o svobodnom obrashchenii takikh dannykh (Obshchii reglament po zashchite dannykh, GDPR).

4. Aziatsko-Tikhookeanskoe ekonomicheskoe sotrudnichestvo (ATES). Sistema transgranichnykh pravil konfidentsial'nosti (CBPR): politika, pravila i rukovodyashchie printsipy. Singapur: Sekretariat ATES, 2019.

5. Organizatsiya ekonomicheskogo sotrudnichestva i razvitiya. Deklaratsiya ob obespechenii gosudarstvami dostupa k personal'nym dannym, khranyashchimsya v chastnom. Parizh: OESR, 14 dek. 2022.

6. Upravlenie po delam kiberprostranstva KNR. Pravila sodeistviya i regulirovaniya transgranichnykh potokov dannykh. Pekin: CAC, 22 marta 2024.

7. Natsional'noe upravlenie po zashchite personal'nykh dannykh Brazilii (ANPD). Rezolyutsiya CD/ANPD №19/2024 o mezhdunarodnoi peredache personal'nykh dannykh. Brazilia: ANPD, 23 avg. 2024.

8. Rossiiskaya Federatsiya. Federal'nyi zakon ot 27 iyulya 2006 g. №152-FZ «O personal'nykh dannykh» (v red. Zakona №420-FZ ot 28 noyab. 2024 g.; s izmeneniyami, vstupayushchimi v silu 1 iyulya 2025 g.). Sobranie zakonodatel'stva Rossiiskoi Federatsii. 2006. №31 (ch. I).

9. Ministerstvo yustitsii SShA. Final'noe pravilo: «Predotvrashchenie dostupa k konfidentsial'nym personal'nym dannym SShA i dannym gosudarstvennogo znacheniya stranami, vyzyvayushchimi ozabochennost', ili sootvetstvuyushchimi litsami» (28 CFR, ch. 202). Vashington: DOJ, 8 apr. 2025.

10. Vsemirnyi ekonomicheskii forum. Svobodnyi potok dannykh s doveriem (DFFT): puti k svobodnym i doveritel'nym potokam dannykh. Zheneva: VEF, 2020.

11. Natsional'nyi sovet po torgovle Shvetsii. Navigating Cross-Border Data Flows and the GDPR: Trade Policy Recommendations. Stokgol'm: Natsional'nyi sovet po torgovle Shvetsii, 2025.

Поступила в редакцию
08.01.2026 г.

Принята к публикации
21.01.2026 г.

Ссылка для цитирования:

Tursunbaeva N., Abolfazl Arab International Standards for Data Protection and Cross-Border Flows // Бюллетень науки и практики. 2026. Т. 12. №3. С. 442-448. https://doi.org/10.33619/2414-2948/124/50

Cite as (APA):

Tursunbaeva, N., & Abolfazl, Arab (2026). International Standards for Data Protection and Cross-Border Flows. *Bulletin of Science and Practice, 12*(3), 442-448. https://doi.org/10.33619/2414-2948/124/50