Global Inventory of Domestic Rules on Data Localization and Data Transfers (2015 - present) [as of January 9, 2023]

This inventory of domestic rules on data localization and data transfers compiles selected laws, regulations, and other measures from the countries listed below. We have selected the most relevant central government measures from privacy and data protection laws in the identified countries. The inventory does not purport to provide a comprehensive listing of all measures containing restrictive cross-border data elements, nor does the inventory include subnational (state, provincial, municipal, or other local) measures. The inventory does not include measures from heavily sanctioned countries, such as Belarus, Cuba, Iran, Myanmar, North Korea, Syria, Russia, or Venezuela. Measures for which English translations could not be located were either: (a) not reviewed; or (b) reviewed in machine-translation only. We have not shepherdized all references, and thus the table may include some legacy measures that may have been superseded to some degree and/or that may retain a limited degree of validity. We intend to update this inventory over time as cross-border data rules are newly proposed, amended, or revoked and/or as we become aware of updated information or other measures not cited herein. We recommend that readers use this inventory only as an indicative guide of relevant cross-border data rules, and refer to original source materials for purposes of any conclusive analysis of legal obligations in particular jurisdictions.

Table of Contents

Albania

Title	Types of Data Covered	Selected Rules in Albania on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	"The international transfer of personal data may be carried out with recipients from states which have an adequate level of personal data protection. The level of personal data protection for a state is established by assessing all circumstances related to the nature, purpose and duration of the processing, the country of origin and final destination, as well as the legal provisions and security standards in force in the recipient state. Pursuant to the Decision of the Commissioner No. 8, dated 31 October 2016 the following states have an adequate level of data protection: • European Union member states; • European Economic Area states; • Parties to the Convention No. 108 of the Council of Europe "For the Protection of Individuals with regard to Automatic Processing of Personal Data", as well as its 1981 Protocol, which have approved a special law and set up a supervisory authority that operates in complete independence, providing appropriate legal mechanisms, including handling complaints, investigating and ensuring the transparency of personal data processing; • States where personal data may be transferred, pursuant to a decision of the European Commission. International transfer of personal data with a state that does not have an adequate level of personal data protection may be done if: • it is authorized by international acts ratified by the Republic of Albania which are directly applicable; • the data subject has given his consent for the international transfer; • the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken in addressing a request of the data subject, or the transfer is necessary for the conclusion or performance of a contract between the controller and a third party, in the interest of the data subject; • it is a legal obligation of the controller; • it is necessary for protecting vital interests of the data subject; • it is necessary or constitutes a legal requirement over an important public interest or for exercising and protecting a legal right; • it is done from a register that is open for consultation and provides information to the general public. Pursuant to the Data Protection Law, the Commissioner issues instructions in order to allow certain categories of personal data to be transferred to a state that does not have an adequate level of personal data protection. In these cases, the controller is exempted from the authorization request. Accordingly, the Commissioner has issued the Instruction No. 41, dated 13 June 2014 "On allowing some categories of international transfers of personal data in a country that does not have an adequate level of personal data protection". Controllers wishing to transfer personal data to other countries lacking adequate personal data protection, may fill in an application form "*For the approval of the transfer of personal data to a state that does not have an adequate level of data protection, through the authorization of the Commissioner*". In 2014, the Commissioner has also issued a Manual on the International Transfer of Personal Data which provides guidelines to the international transfer of personal data.	DLA Piper, *Data Protection Laws of the World*
REPUBLIC OF ALBANIA THE ASSEMBLY LAW No. 9887 dated	Personal	Excerpt **Article 8** International transfer (Amended point 1, point 2 letter "c" with law no.48/2012)	

10.03.2008 ON PROTECTION OF PERSONAL DATA (Amended by the Law No. 48/2012, date 26.04.2012) (Amended by the Law No.120/2014)		1. The international transfer of personal data is done with recipients from states which have an adequate level of personal data protection. The level of personal data protection for a state is established by assessing all circumstances related to processing, nature, purpose and duration of processing, country of origin and final destination, legal provisions and security standards in force in the recipient state. States that have an adequate level of data protection are assessed under a decision of the Commissioner. 2. International transfer of personal data with a state that does not have an adequate level of personal data protection may be done when: a) it is authorised by international acts ratified by the Republic of Albania and are directly applicable; b) data subject has given his/her consent for the inter-national transfer; c)the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken in addressing the data subject's request, or the transfer is necessary for the conclusion or performance of a contract between the controller and a third party, in the interest of the data subject; ç) it is a legal obligation of the controller; d) it is necessary for protecting vital interests of the data subject; dh) it is necessary or constitutes a legal requirement over an important public interest or for exercising and protecting a legal right; e)transfer is done from a register that is open for consultation and provides information to the general public. 3. Exchange of personal data to the diplomatic representations of foreign governments or international institutions in the Republic of Albania shall be considered an international transfer of data. **Article 9** International transfer of data that need to be authorized (Added words point 1, point 2 with law no.48/2012) 1. In cases other than those provided for in Article 8 herein, the international transfer of personal data with a state that does not have an adequate level of data protection, shall be carried out upon an authorization from the Commissioner, if adequate safeguards are foreseen with respect to the protection of the privacy and fundamental human rights and freedoms, as well as regarding the exercise of the corresponding rights. 2. The Commissioner, after making an assessment, under the specification provided in point 1 of this Article and point 1 of Article 8 may give the authorization for transfer of personal data to the recipient State by defining conditions and obligations. 3. The Commissioner issues instructions in order to allow certain categories of personal data international transfer to a state that does not have an adequate level of personal data protection. In these cases, the controller is exempted from the authorization request. 4. The controller shall submit a request for authorisation to the Commissioner prior to the data transfer. In the authorization request, the controller shall guarantee the observance of the interests of the data subject to protection of confidentiality outside the Republic of Albania. https://www.idp.al/wp-content/uploads/2019/10/LDP_english_version_amended_2014.pdf	

Algeria

Title	Types of Data Covered	Selected Rules in Algeria on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The data controller may only transfer personal data to a foreign State with the authorisation of the national authority in accordance with Law No. 18-07 and if that State ensures an adequate level of protection of the privacy and fundamental rights and freedoms of individuals with regard to the processing of such data. In any case, it is forbidden to communicate or transfer personal data to a foreign country, when such transfer is likely to affect public security or the vital interests of the State. However, as the national authority has not yet been established, the consent of the data subject is required.	DLA Piper, *Data Protection Laws of the World,* at: https://www.dlapiperdataprotection.com/index.html?t=transfer&c=DZ&c2=
Law on the Protection of Natural Persons In Regard to the Processing of Personal Data (Law No. 18-07 of 25 Ramadhan 1439 corresponding to the 10 June 2018)	Personal	Excerpt (machine translation): Transfer of data to a foreign country **Art. 44.** — The controller may not transfer, personal data to a foreign State, except with the authorization of the national authority, in accordance with the provisions of this Act and only if that State shall ensure an adequate level of protection of life privacy and fundamental rights and freedoms of individuals with regard to the processing to which such data are subjected, or may be the subject. The sufficiency of the level of protection provided by a State is assessed by the national authority in particular, in depending on the legal provisions in force in that State, the security measures applicable thereto, specific characteristics of the processing such as its purposes and its duration, as well as the nature, origin and destination of the processed data. It is prohibited, in any case, to communicate or transfer personal data to a foreign country, where such transfer is likely to affect harm to public safety or the vital interests of the State. **Art. 45**. — By way of derogation from Article 44 of this Act, the controller may transfer personal data to a State not meeting the conditions laid down in that Article: (1) if the person concerned has expressly consented to their transfer; (2) if the transfer is necessary, (a) the safety of that person's life; (b) the preservation of the public interest; (c) compliance with obligations to ensure the the establishment, exercise or defence of legal claims; (d) the performance of a contract between the person responsible for the processing and the data subject, or measures pre-contractual taken at the request of the latter; (e) the conclusion or performance of a contract concluded, or to be concluded, in the interest of the data subject, between the controller and a third party; (f) the execution of a mutual legal assistance measure international; (g) prevention, diagnosis or treatment medical conditions (3) if the transfer is made pursuant to an agreement bilateral or multilateral to which Algeria is a party; (4) with the authorization of the national authority, if the processing complies with the provisions of Article 2 of the this Act. **Art. 67**. — Is punishable by imprisonment of one (1) year to five (5) years and a fine of 500,000 DA to 1,000.000 DA, anyone who makes a data transfer of a personal nature to a foreign State, in violation of the provisions of section 44 of this Act.	Algeria Official Gazette, *Law on the Protection of Natural Persons In Regard to the Processing of Personal Data* OneTrust, *Algeria Summary* https://www.joradp.dz/Jo2000/2018/034/FP10.pdf

Andorra

Title	Types of Data Covered	Selected Rules in Andorra on Cross-Border Data Transfers or Data Localization	Sources
Qualified law 15/2003 on personal data protection	Personal	Excerpt (machine translation) Chapter six. International communication of data **Article 35** - Requirements for the international communication of data No international data communication may be effected unless the current regulations in the country of destination establish a level of personal data protection at least equivalent to that established in this Act. **Article 36** - Countries with equivalent protection It is understood that the following have a level of protection equivalent to this Act: a) Member countries of the European Union. b) Countries declared by the European Communities Commission as countries with protection equivalent. c) Countries declared as such by the Andorran Data Protection Agency. **Article 37** - Exceptions The prohibition established in article 35 of this Act does not apply when the international communication: a) Is made with the unequivocal consent of the interested party. b) Is made in accordance with international conventions of which the Principality Andorra is a party. c) Is made for the purposes of international legal assistance, or for the recognition, exercise or defence of a right in the context of legal proceedings. d) Is made for medical prevention or diagnosis, health care, social prevention or diagnosis or for the vital interest of the interested party. e) Is made for the purpose of bank remittances or transfers of money. f) Is necessary for the establishment, execution, fulfilment or control of legal relationships or contractual obligations between the interested party and the file manager. g) Is necessary to preserve the public interest. h) Is concerned with data taken from public registries or is made in compliance with the functions and purposes of the public registries.	https://www.afapdp.org/wp-content/uploads/2018/05/Andorre-Loi-n%C2%B015-2003-relative-a-la-protection-des-donnees-personnelles-2003.pdf

Angola

Title	Types of Data Covered	Selected Rules in Angola on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Angola regulates data privacy and protection issues under the Data Protection Law (Law no. 22/11, 17 June 2011), the Electronic Communications and Information Society Services Law (Law no. 23/11, 20 June 2011) and the Protection of Information Systems and Networks Law (Law no. 7/17, 16 February 2017) International transfers of personal data to countries with an adequate level of protection require prior notification to the Agência de Proteção de Dados (APD). An adequate level of protection is understood as a level of protection equal to the Angolan Data Protection Law. APD decides which countries ensure an adequate level of protection by issuing an opinion to this respect. International transfers of personal data to countries that do not ensure an adequate level of protection are subject to prior authorization from the APD, which will only be granted if specific requirements are met. For transfers between companies in the same group, the requirement of an adequate level of protection may be reached through the adoption of harmonized and mandatory internal rules on data protection and privacy. Please note that the communication of personal data to a recipient, a third party or a subcontracted entity is subject to specific legal conditions and requirements.	DLA Piper, *Data Protection Laws of the World*, at: https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all
Data Protection Law (Law no. 22/11, 17 June 2011)	Personal	Excerpt (machine translation) Data Protection Law (Law no. 22/11, 17 June 2011) **SECTION VI - International Transfer of Personal Data** **ARTICLE 33** (Transfer of data to countries that ensure a level of adequate protection) 1. The international transfer of data to countries that ensure an adequate level of protection is subject to notification to the Data Protection Agency. 2. It is understood that a country ensures an adequate level of protection when it guarantees, at least, a level of protection equal to that established in this law. 3. It is up to the Data Protection Agency to decide whether a State ensures an adequate level of protection, by issuing an opinion in this regard. 4. The adequacy of the level of data protection in a State is assessed by the Data Protection Agency according to all the circumstances surrounding the transfer or set of data transfers, taking into account in particular the nature of the data, the purpose and the duration of the treatment or treatments envisaged, the countries of final destination and the general or sectoral rules of law in force in the State concerned, including the professional rules and security measures that are respected in that State. **ARTICLE 34** (Data transfer to countries that do not follow an adequate level of protection) 1. The international transfer of data to a country that does not guarantee an adequate level of protection is subject to authorization from a data protection agency, which can only be granted if one of the following circumstances or other specific legislation is verified: a) if the data subject has given his unequivocal, express and written consent b) if the international transfer of data results from the application of international treaties or agreements to which the Republic of Angola is a party if the international transfer of data results from the application of international treaties or agreements to which the Republic of Angola is a party c) if the transfer of data is for the sole purpose of responding to or requesting humanitarian assistance d) if the transfer of data is necessary for the performance of a contract between the data subject and the person responsible for the treatment or steps prior to the formation of the contract decided at the request of the data subject e) if the transfer of data is necessary for the performance or conclusion of a contract, in the interest of the data subject, between the data controller and a third party f) if the transfer of data is necessary or legally required for the protection of an important public interest or for the declaration, exercise or defense of a right in legal proceedings g) if the transfer of data is necessary to protect the vital interests of the data subject, or for prevention, diagnosis or medical treatment and the subject is physically or legally unable to give consent	https://media2.mofo.com/documents/Law_22_11_Data_Privacy_Law.pdf

Title	Types of Data Covered	Selected Rules in Angola on Cross-Border Data Transfers or Data Localization	Sources
		h) if the data transfer is from a publicly accessible source i) if the recipient of the data contractually guarantees, before the person responsible for the treatment, an adequate level of protection for the transferred data 2. It is up to the data protection agency to determine the specific conditions that must be included in the contract referred to in paragraph i) of the previous number 3. In the case of international data transfer between companies of the same business group, the guarantee of compliance with an adequate level of protection can be achieved through the adoption of uniform internal rules regarding privacy and data protection whose compliance is mandatory. **SECTION VII Formalities for Notification and Obtaining Authorization with the Data Protection Agency** **ARTICLE 35**. (Obligation to notify or obtain authorization) 1. Without prejudice to the provisions of this law, the processing of personal data is subject to prior notification to the Data Protection Agency or its authorization. 2. If mere notification is required, the Data Protection Agency must issue an opinion on the data controller's request within thirty days of receipt, at the end of which it is understood that the treatment has been duly notified. 3. The Data Protection Agency may authorize the simplification or exemption of notification for certain categories of treatment that, given the specificity of the data, are not likely to jeopardize the rights, guarantees and fundamental freedoms of data subjects, and taking into account criteria of celerity , economy and efficiency. 4. The exemption authorization must, among other aspects, specify the purposes of the treatment, the data or categories of data to be processed, the category or categories of data subjects, the recipients or categories of recipients to whom the data may be communicated and the period of data conservation. 5. Treatments whose sole purpose is the maintenance of records that are intended for public information and can be consulted by the general public or by any person who proves a legitimate interest are exempt from notification. 6. Obtaining authorization from the Data Protection Agency is waived if the treatment results from a legal diploma, in which case it is sufficient to proceed with mere notification, unless otherwise indicated in specific legislation.	

Argentina

Title	Types of Data Covered	Selected Rules in Argentina on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Transfers and disclosures to third parties Personal data may only be transferred for legitimate purposes of the transferor and the transferee, and generally with the prior consent of the data subject who must be informed of the transfer's purpose and of the transferee's identity. This consent may be rescinded. Consent is not required in the case of transfer of data regarding which consent was not necessary for collection. Also, it is not necessary in the case of transfer of data between state agencies, for purposes of performance of their respective activities, on in connection with health-related data, if the transfer is necessary for public health or emergency reasons, or for the performance of epidemiological studies, provided the identity of the persons to whom such data refer is reserved by means of adequate dissociation mechanism. In addition, consent is not necessary, for personal data generally, if an adequate dissociation mechanism is used in a way such that the data subjects are not identifiable. Cross-border transfers The cross-border transfer of personal data is prohibited to countries or international or supranational organization which do not provide adequate protection to such data, unless: • The data subjects expressly consents to that transfer • The transfer is necessary for international judicial cooperation • The transfer takes place as part of certain exchanges of medical data • Bank or stock exchange transfers, in the context banking or stock exchange transactions • The transfer takes place as provided in the context of international treaties to which Argentina is a party • The transfer has as its purpose the international cooperation between intelligence agencies engaged in combating organized crime, terrorism and drug traffic	DLA Piper, *Data Protection Laws of the World*, at: https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all

Personal Data Protection Bill (Oct. 11, 2022)	Personal	ARTICLE 16. - Information to be Provided to the Data Subject. The Data Controller must provide the Data Subject, before collection, in a concise, transparent manner, intelligible and easily accessible, with clear and simple language, at least the following information: ... f) information on international data transfers, with inclusion of destination countries, identity and contact details of the recipient, possible risks associated with applicable transfers and safeguards, categories of data involved, purpose and mechanisms to exercise their rights… Chapter 3 International transfers ARTICLE 23. - General principle of international transfers. Transfers of personal data outside the national territory, including onward transfers, may be performed in any of the following cases: (a) If the recipient international organization or body provides an adequate level of protection; (b) If the exporter offers appropriate guarantees for the processing of personal data, in compliance with the minimum and sufficient conditions laid down in this law; (c) Pursuant to derogations for specific situations specified in Article 25 of this Law. In order to demonstrate that the international transfer is made in accordance with the provisions of this Law, the burden of proof lies, in all cases, with the exporter. Whoever performs an international data transfer must implement measures to guarantee the rights of the data subject and must respond to any potential breach [of those rights]. ARTICLE 24. - International transfers based on an adequacy decision. The implementing authority shall determine the appropriate country status, taking into account the following elements: (a) The rule of law, respect for human rights and fundametal freedoms; (b) existing legislation, both general and sectoral, including limitations and guarantees for public authorities' access to personal data; (c) the existence of judicial and institutional guarantees for the observance of rights to the protection of personal data; (d) the existence and effective functioning of one or more authorities of independent control in the country or organisation receiving the information, with the responsibility for ensuring and enforcing standards for the protection of data, including appropriate enforcement powers, to assist and advise data subjects in the exercise of their rights, and to cooperate with the Enforcement Authority. ARTICLE 25. - International transfers through adequate guarantees. In the absence of an adequacy decision, adequate guarantees can be provided by: (a) a legally binding and enforceable instrument between authorities, or public bodies of the ARGENTINE REPUBLIC and other countries, containing the principles, rights and obligations established in this Law; (b) a bilateral or multilateral international agreement, between the ARGENTINE REPUBLIC and other countries or international organizations, containing the principles, Obligations and rights established in this law, and that enables transfers from private and/or public entities established in Argentina to private entities and/or public established in other countries; (c) agreements or arrangements expressly recognising the principles, rights and obligations established in this law, which may be adopted in the following ways: I. Model contractual clauses that have been previously approved by the Enforcement Authority; II. Binding corporate rules that have been approved by the Enforcement Authority and which apply to all members of an economic group under the terms established by this law; III. Data protection certification mechanisms approved by the Enforcement Authority. In the case of transfers governed by this Article, the agreement or mechanism that implements the transfer must recognize that the exporting party is subject to the jurisdiction of the Enforcement Authority and the competency of the courts of the ARGENTINE REPUBLIC, and ensure that the importing party is subject to the jurisdiction of one or more independent supervisory authorities so that data subjects have effective legal recourse to protect their rights. ARTICLE 26. -Exceptions. International transfers can be made exceptionally if any of the following conditions are met: (a) that the Data Subject has given his consent; (b) the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller, or for the benefit of the Data Controller data, between the Data Controller and another human or legal person, or for the execution of pre-contractual measures adopted at the request of the Data Subject; (c) the transfer is necessary: (I) for reasons of public interest; (II) for the recognition, exercise or defense of a right in a judicial process; or (III) to protect the vital interests of the Data Subject or other persons, if physically or legally incapable of giving consent.	Argentine Agency for Access to Public Information, Personal Data Protection Bill, https://www.argentina.gob.ar/sites/default/files/proyecto_de_ley_de_datos_personales_aaip.pdf ; New Personal Data Protection Bill | Argentina.gob.ar

		The conditions laid down in this Article should always be subject to compliance with international human rights standards applicable to the matter, to compliance with the principles of this law and to the criteria of legality, proportionality and necessity. The exceptions listed herein cannot be used to make periodic or habitual international transfers, or transfers involving a large number of people.	
Personal Data Protection Act, Act 25.326 (Oct. 4, 2000)	Personal	Excerpt **SECTION 12**.- International transfer 1.- The transfer of any type of personal information to countries or international or supranational entities which do not provide adequate levels of protection, is prohibited. 2.- The prohibition shall not apply in the following circumstances: a) international judicial cooperation; b) exchange of medical information, when so required for the treatment of the party affected, or in case of an epidemiological survey, provided that it is conducted in pursuance of the terms of Paragraph e) of the foregoing Section; c) stock exchange or banking transfers, to the extent thereof, and in pursuance of the applicable laws; d) when the transfer is arranged within the framework of international treaties which the Argentine Republic is a signatory to; e) when the transfer is made for international cooperation purposes between intelligence agencies in the fight against organized crime, terrorism and drug-trafficking.	Argentina, *Personal Data Protection Act* DATA PROTECTION (infoleg.gob.ar)

Armenia

Title	Types of Data Covered	Selected Rules in Armenia on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Transfer to third parties shall mean an operation aimed at transferring personal data to certain scope of persons or public at large or at familiarising with them, including disclosure of personal data through the mass media, posting in information communication networks or otherwise making personal data available to another person. The processor may transfer personal data to third parties or grant access to data without the personal data subject's consent, where it is provided for by law and has an adequate level of protection. The processor may transfer special category personal data to third parties or grant access to data without the personal data subject's consent, where: • the data processor is considered as a processor of special category personal data prescribed by law or an interstate agreement, the transfer of such information is directly provided for by law and has an adequate level of protection; • in exceptional cases provided for by law special category personal data may be transferred for protecting life, health or freedom of the data subject. Personal data may be transferred to another country with the data subject's consent or where the transfer of data stems from the purposes of processing personal data and/or is necessary for the implementation of these purposes. Personal data may be transferred to another state without the permission of the authorised body, where the given state ensures an adequate level of protection of personal data.	DLA Piper, *Data Protection Laws of the World*, at: https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all
Law of the Republic of Armenia on Protection of Personal Data (June 13, 2015)	Personal	Excerpt **Article 27**. Transfer of personal data to other states 1. Personal data may be transferred to other country by the data subject's consent or where the transfer of data stems from the purposes of processing personal data and/or is necessary for the implementation of these purposes. 2. Personal data may be transferred to other state without the permission of the authorised body, where the given State ensures an adequate level of protection of personal data. An adequate level of protection of personal data shall be considered to be ensured, where: (1) personal data are transferred in compliance with international agreements; (2) personal data are transferred to any of the country included in the list officially published by the authorised body. 3. Personal data may be transferred to the territory of the State not ensuring an adequate level of protection only by the permission of the authorised body where personal data are transferred on the basis of an agreement, and the agreement provides for such safeguards with regard to the protection of personal data which were approved by the authorised body as ensuring adequate protection. 4. In cases referred to in part 3 of this Article the processor of personal data shall be obliged— prior to the transfer of data to other country — apply to the authorised body to obtain permission. The processor of personal data shall be obliged to specify in the application the country where personal data are transferred, the description of the recipient of personal data (name, legal form), description (content) of personal data, purpose of processing and transferring personal data, agreement or the draft thereof. The authorised body shall be obliged to permit or reject the application within 30 days. The authorised body may require from the processor of personal data additional information by observing the time limit for the consideration of the application. In case when the authorised body finds that contractual safeguards are not sufficient, it shall be obliged to specify those necessary changes which will ensure safeguards for the protection of personal data. 5. The authorised body for the protection of personal data, regularly but not less than once in a year, shall be obliged to revise the list of countries ensuring an adequate level of protection of personal data and publish the changes in the official journal and in its official website. 6. Personal data under the disposition of state bodies may be transferred to foreign state bodies only within the scope of interstate agreements, whereas to non-state bodies in accordance with the norms of this Article.	Personaldataprotectionlaw_ENG.pdf (foi.am)

Title	Types of Data Covered	Selected Rules in Armenia on Cross-Border Data Transfers or Data Localization	Sources

Australia

Title	Types of Data Covered	Selected Rules in Australia on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Unless certain limited exemptions under the Privacy Act apply, personal information may only be disclosed to an organization outside of Australia where the entity has taken reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the personal information. The disclosing / transferring entity will generally remain liable for any act(s) done or omissions by that overseas recipient that would, if done by the disclosing organization in Australia, constitute a breach of the APPs. However, this provision will not apply where any of the following apply: • The organization reasonably believes that the recipient of the information is subject to a law or binding scheme which effectively provides for a level of protection that is at least substantially similar to the Privacy Act, including as to access to mechanisms by the individual to take action to enforce the protections of that law or binding scheme. There can be no reliance on contractual provisions requiring the overseas entity to comply with the APPs to avoid ongoing liability (although the use of appropriate contractual provisions is a step towards ensuring compliance with the 'reasonable steps' requirement). • The individual consents to the transfer. However, under the Privacy Act the organization must, prior to receiving consent, expressly inform the individual that if he or she consents to the overseas disclosure of the information the organization will not be required to take reasonable steps to ensure the overseas recipient does not breach the APPs. • A 'permitted general situation' applies. • The disclosure is required or authorized by law or a court/tribunal order.	DLA Piper, *Data Protection Laws of the World*, at: https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all
Privacy Act 1988 No. 119, 1988 (including retrospective amendments made by Act No. 197, 2012 as amended by Act No 5, 2015)	Personal	Excerpt **Schedule 1—Australian Privacy Principles** **Part 3—Dealing with personal information** 8 Australian Privacy Principle 8—cross-border disclosure of personal information 8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient): (a) who is not in Australia or an external Territory; and (b) who is not the entity or the individual; the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information. Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles. 8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if: (a) the entity reasonably believes that: (i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and (ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or (b) both of the following apply: (i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure; (ii) after being so informed, the individual consents to the disclosure; or (c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or	Personaldataprotectionlaw_ENG.pdf (foi.am)

Title	Types of Data Covered	Selected Rules in Australia on Cross-Border Data Transfers or Data Localization	Sources
		(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or (e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or (f) the entity is an agency and both of the following apply: (i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; (ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body. Note: For permitted general situation, see section 16A.	

Austria

Title	Types of Data Covered	Selected Rules in Austria on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Azerbaijan

Title	Types of Data Covered	Selected Rules in Azerbaijan on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Under the Law on Personal Information dated 11 May 2010, transfer of personal data can be performed with a prior written consent of a data subject, unless the data is of open category.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=AZ
Law of 11 May 2010 No. 998-IIIQ on Personal Data (only available in Azerbaijani)	Personal	Not summarized due to lack of translation.	http://www.e-qanun.az/framework/19675

Bahamas

Title	Types of Data Covered	Selected Rules in Bahamas on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Section 17 of the Data Protection Act (DPA) speaks to the international transfer of data. Under Section 17(1) the DPC may prohibit the transfer of personal data from The Bahamas to a place outside The Bahamas in cases where there is a failure to provide protection either by contract or otherwise equivalent to that provided under DPA, subject to certain exceptions. In arriving at a determination to prohibit the international transfer of data, the DPC must consider whether such a transfer would cause damage or distress to any person and consider the desirability of the transfer. Pursuant to Section 17(8) however, data constituting data required or authorized to be transferred under another enactment; or data that is required by any convention or other instrument imposing an international obligation on The Bahamas; or otherwise, data that a data subject has consented to having transferred, will not apply under Section 17.	https://www.dlapiperdataprotection.com/index.html?t=law&c=BS
Data Protection (Privacy of Personal Information) Act 2003	Personal	Excerpt Prohibition on transfer of personal data outside The Bahamas **17**. (1) The Commissioner may, subject to the provisions of this section, prohibit the transfer of personal data from The Bahamas to a place outside The Bahamas, in such cases where there is a failure to provide protection either by contract or otherwise equivalent to that provided under this Act. (2) In determining whether to prohibit a transfer of personal data under this section, the Commissioner shall also consider whether the transfer would be likely to cause damage or distress to any person and have regard to the desirability of facilitating international transfers of data. (3) A prohibition under subsection (1) shall be effected by the service of a notice (referred to in this Act as a prohibition notice) on the person proposing to transfer the data concerned. (4) A prohibition notice shall — (a) prohibit the transfer concerned either absolutely or until the person aforesaid has taken such steps as are specified in the notice for protecting the interests of the data subjects concerned; (b) specify the time when it is to take effect; (c) specify the grounds for the prohibition; and (d) subject to subsection (6), state that the person concerned may appeal to the Court under section 24 against the prohibition specified in the notice within twenty-one days from the service of the notice on him. (5) Subject to subsection (6), the time specified in a prohibition notice for compliance with the prohibition specified therein shall not be expressed to expire before the end of the period of the twenty-one days specified in subsection (4)(d) and, if an appeal is brought against the prohibition, the prohibition need not be complied with and subsection (10) shall not apply in relation thereto, pending the determination or withdrawal of the appeal. (6) If the Commissioner — (a) by reason of special circumstances, is of the opinion that a prohibition specified in a prohibition notice should be complied with urgently; and (b) such prohibition notice includes a statement to that effect, subsections (4)(d) and (5) shall not apply in relation to the notice but the notice shall contain a statement of the effect of the provisions of section 24 (other than subsection (2)) and shall not require compliance with the prohibition before the end of the period of seven days beginning on the date on which the notice is served. (7) The Commissioner may cancel a prohibition notice and, if he does so, shall notify in writing the person on whom it was served accordingly. (8) This section shall not apply to a transfer of data if the transfer of the data or the information constituting the data is required or authorised by or under any enactment, or required by any convention or other instrument imposing an international obligation on The Bahamas, or otherwise made pursuant to the consent (express or implied) of the data subjects.	http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0003/DataProtectionPrivacyofPersonalInformationAct_1.pdf

Title	Types of Data Covered	Selected Rules in Bahamas on Cross-Border Data Transfers or Data Localization	Sources
		(9) This section applies, with any necessary modifications, to a transfer of information from The Bahamas to a place outside The Bahamas for conversion into personal data as it applies to a transfer of personal data from The Bahamas to such a place; and in this subsection “information” means information (not being data) relating to a living individual who can be identified from it. (10) A person who, without reasonable excuse, fails or refuses to comply with a prohibition specified in a prohibition notice shall be guilty of an offence	

Bahrain

Title	Types of Data Covered	Selected Rules in Bahrain on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Bahrain enacted Law No. 30 of 2018 with respect to Personal Data Protection ("PDPL") on July 12, 2018. Transfers of personal data out of Bahrain is prohibited unless the transfer is made to a country or region that provides sufficient protection to personal data. Those countries need to be listed by the Authority and published in the Official Gazette. Data controllers can also transfer personal data to countries that are not determined to have sufficient protection of personal data where: • the transfer occurs pursuant to a permission to be issued by the Authority on a case-by-case basis, if it deems that the data will be sufficiently protected; • if the data subject has consented to that transfer; • if the data to be transferred has been extracted from a register that was created in accordance with the PDPL for the purpose of providing information to the public, regardless of whether viewing of this register is available to everyone or limited to the parties concerned in accordance with specific terms and conditions. In this instance, one shall have to satisfy the terms and conditions prescribed for viewing the register before viewing that information; • if the transfer is necessary for any of the following: o to implement a contract between the data subject and the data controller, or to undertake preceding steps at the data subject's request for the purpose of concluding a contract; o to implement or conclude a contract between the data controller and a third party for the benefit of the data subject; o to protect the data subject's vital interests; o to implement an obligation imposed by the PDPL (even if this is contrary to the contractual obligation), or to implement an order issued by a competent court, the public prosecution, the investigating judge or the military prosecution; or o to prepare, execute or defend a legal claim.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=BH
Law No. (30) of 2018 with Respect to Personal Data Protection Law	Personal	Excerpt (translated version) **Section Three** - Transfer of Personal Data outside the Kingdom **Article (12)** - Transfer of personal data to countries or territories with adequate protection The Data Controller is prohibited from transferring personal data outside the Kingdom, except for the following cases: 1- The transfer is to a country or territory that is listed in a record compiled and updated by the Authority, comprising of countries and territories that, upon the Authority's discretion, provide adequate legislative and regulatory protection for personal data. Such record shall be published in the Official Gazette. 2- A transfer occurs upon the Authority's authorisation on a case-by-case basis provided that the data will be subject to an adequate level of protection. The adequacy of such level of protection shall be assessed in the light of all the circumstances surrounding the data transfer operation, which shall include in particular the following: i. the nature of the data to be transferred, purpose and duration of processing; ii. the country or territory of origin of the data, its final destination, and available measures, in such countries and territories, to protect personal data; and iii. Relevant international agreements and legislations that are in force in the country or territory, which the data shall be transferred to. The aforementioned authorisation may be conditional or for a certain timeframe. **Article (13)** - Exemptions 1- Notwithstanding the provisions of Article (12) of this Law, the Data Controller may transfer personal data outside the Kingdom to another country or territory that does not provide adequate level of protection in any of the following circumstances: a - if the data subject has given his consent to the transfer; b - If the transfer is for data obtained from a register compiled in accordance with the law for the purpose of providing information to the public, whether it is available for the public or limited to any person demonstrating a legitimate interest, in accordance with certain conditions. In such case, accessing this information shall be in accordance with stipulated conditions concerning accessing the register. c - If the transfer is necessary for:	https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.legalaffairs.gov.bh%2FFullEn%2FK3018.docx&wdOrigin=BROWSELINK

Title	Types of Data Covered	Selected Rules in Bahrain on Cross-Border Data Transfers or Data Localization	Sources
		1. the performance of a contract between the data subject and the Data Controller or taking steps, at the request of the data subject, with the purpose of entering into a contract; 2. the conclusion or performance of a contract entered into, in the interest of the data subject, between the Data Controller and a third party; 3. protecting the vital interests of the data subject; 4. Complying with an obligation prescribed in law, not being a contractual obligation, or complying with an order from a competent court, the Public Prosecution, the investigation Judge, or the Military Prosecution; or 5. Preparing or pursuing a legal claim or defense. 2- Without prejudice to Paragraph (1) of this Article, the Authority may authorize a transfer of personal data, or collection thereof, to another country or territory that does not ensure an adequate level of protection within the meaning of Article (12) of this Law, where the Data Controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals. These safeguards may –in particular- be prescribed according to a contract to which the Data controller is a party, and the Authority shall accordingly subject the grant of such authorisation to fulfilment of certain conditions.	

Bangladesh

Title	Types of Data Covered	Selected Rules in Bangladesh on Cross-Border Data Transfers or Data Localization	Sources
DRAFT Data Protection Act (July 16, 2022)	Personal	CHAPTER X: PROVISIONS RELATING TO STORAGE AND TRANSFER OF DATA 42. Storage of sensitive data, user created or generated data and classified data. The sensitive data, user created or generated data and classified data shall be stored in Bangladesh, and shall remain beyond the jurisdiction of any court and law enforcers other than Bangladesh. 43. Transfer of data as mentioned in section 42. (1) Any classified data specified by the Government, from time to time, by general or special order, may not be transferred to a place or system outside Bangladesh if it is not authorized so by the Government. (2) Notwithstanding anything contained in any other provisions of this Act- (a) a data subject by his consent to meet his necessity, may transfer any data including sensitive and user created data, (b) for the purpose of maintaining international relations, cross-border business, immigration or any other data as specified by the Government, from time to time, may transfer any data, to any country or organization outside Bangladesh or international organizations.	Bangladesh, Data Protection Act 2022
Bank Companies Act	Financial data	Section I2 of the Bank Companies Act, I 99 I has imposed a restriction upon bank companies with regard to removal of documents and records outside Bangladesh without prior permission of Bangladesh Bank (i.e. the central bank of Bangladesh). The requirement for obtaining prior written permission from Bangladesh Bank is upon the transferor, i.e. the bank company. Banks must also maintain confidentiality in banking transactions.	Transfer in Bangladesh - DLA Piper Global Data Protection Laws of the World (dlapiperdataprotection.com)
BTRC licensing requirements	Telecom data	The Bangladesh Telecommunication Regulatory Commission ("**Commission**") is the authority that is responsible for regulating telecommunications companies ("**telcos**") in Bangladesh and issuing licenses to telcos for providing mobile phone services. The license which is granted to the telcos contains a provision regarding subscriber confidentiality. The confidentiality requirement applies to *"all information provided by the subscriber"*. As such, telcos will be prohibited from sharing any subscriber information (to entities or persons located inside or outside Bangladesh) that does not come within the exemptions listed above. Furthermore, in our opinion, subscribers would not have the option of giving consent to the telcos to share their data, instead for such sharing, approval from the Commission will be required.	Transfer in Bangladesh - DLA Piper Global Data Protection Laws of the World (dlapiperdataprotection.com)
Comments to the People's Republic of Bangladesh on The Draft Cloud Computing Policy May 2021	Various	Excerpt: II. Cross-Border Data Restrictions in the Draft Cloud Computing Policy Under the heading, "Data Storage Location," the draft Cloud Computing Policy states as follows: The primary location of cloud service provider's data storage must be in Bangladesh. Information may be allowed to be taken outside Bangladesh for back-up and retrieval purposes where the such (sic.) information do not have any personal, sensitive or any such information and information whichis not harmful to the security and critical information infrastructure of Bangladesh. All that information should be hosted in those countries where the Government of Bangladesh has multilateral or bilateral relations for unconditional and instantaneous laws can prevail.	Global Data Alliance, Comments to the People's Republic of Bangladesh on The Draft Cloud Computing Policy (May 2021)

Barbados

Title	Types of Data Covered	Selected Rules in Barbados on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The Data Protection Act (the "**Act"**) was passed on August 12, 2019, and came into force in March 2021. The purpose of the Act is to regulate the collection keeping, processing, use and dissemination of personal data and to protect the privacy of individuals in relation to their personal data. Transfer of personal data is unlawful unless certain conditions are satisfied. Where the data subject has given their consent to the transfer of their personal data, the restrictions on the transfer of the data do not apply. The Act also sets out various other exemptions for the restrictions where transfer of the personal data is necessary e.g. for the performance of a contract between the data subject and the data controller, reasons of substantial public interest, for the purpose of obtaining legal advice, etc. Personal data obtained must not be transferred to a country or territory outside Barbados unless that country or territory provides for (a) an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data and (b) appropriate safeguards on condition that the rights of the data subject are enforceable and there are available, effective legal remedies for data subjects. The circumstances for determining an adequate level of protection as well as methods for providing appropriate safeguards including the development of binding corporate rules must submitted to the Commissioner for authorisation. The "*binding corporate rules*" must specify (but not limited to) the following: • the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members; • the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question; • their legally binding nature, both in and outside of Barbados.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=BB
DATA PROTECTION ACT, 2019	Personal	Excerpt **PART IV - TRANSFERS OF PERSONAL DATA OUTSIDE OF BARBADOS** **General principle for transfers** **22**. Personal data shall not be transferred to a country or territory outside Barbados unless that country or territory provides for (a) an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data; and (b) appropriate safeguards on condition that the rights of the data subject are enforceable and there are available, effective legal remedies for data subjects. **Adequate level of protection** **23.** For the purposes of section 22, an adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to (a) the nature of the personal data; (b) the country or territory of origin of the information contained in the data; (c) the country or territory of final destination of that information; (d) the purposes for which and period during which the data is intended to be processed; (e) the law in force in the country or territory in question; (f) the international obligations of that country or territory; (g) any relevant codes of conduct or other rules which are enforceable in that country or territory whether generally or by arrangement in particular cases; and (h) any security measures taken in respect of the data in that country or territory. **Appropriate safeguards** **24.** For the purposes of section 22, appropriate safeguards may be provided for by (a) a legally binding and enforceable instrument between public authorities; (b) binding corporate rules in accordance with section 25; (c) standard data protection clauses prescribed by the Commissioner with the approval of the Minister; (d) contractual clauses authorised by the Commissioner between the data controller or data processor and the data controller, data processor or the recipient of the personal data; or (e) provisions, authorised by the Commissioner, to be inserted into administrative arrangements between public authorities which include enforceable and effective data subject rights.	https://www.barbadosparliament.com/uploads/bill_resolution/7b81b59260896178b5aa976fdb87bfee.pdf

Title	Types of Data Covered	Selected Rules in Barbados on Cross-Border Data Transfers or Data Localization	Sources
		Binding corporate rules **25.** (1) Data controllers and data processors shall develop binding corporate rules which shall specify (a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members; (b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question; (c) their legally binding nature, both in and outside of Barbados; (d) the application of principles regarding purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of sensitive personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules; (e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with this Act, the right to lodge a complaint with the competent supervisory authority or Commissioner and the High Court and to obtain any other available form of redress and, where appropriate, compensation for a breach of the binding corporate rules; (f) the acceptance by the data controller or data processor of liability for any breaches of the binding corporate rules; (g) that the data controller or the data processor shall be exempt from the liability referred to in paragraph (f), in whole or in part, only where it is proven that the data controller or data processor is not responsible for the event giving rise to the damage; (h) how the information on the binding corporate rules is provided to the data subjects; (i) the complaint procedures; (j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules; (k) the mechanisms for reporting and recording changes to the binding corporate rules and reporting those changes to the supervisory authority; (l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority or Commissioner the results of verifications of the measures specified in paragraph (j); (m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and (n) the appropriate data protection training to personnel having permanent or regular access to personal data. (2) The binding corporate rules referred to in subsection (1) shall be submitted to the Commissioner for authorisation. (3) The Commissioner may specify the format and procedures for the exchange of information between data controllers, data processors and supervisory authorities for binding corporate rules. **Derogations** **26.** Section 22, 23 and 24 shall not apply where (a) the data subject has given his consent to the transfer of personal data; (b) the transfer of personal data is necessary for (i) the performance of a contract between the data subject and the data controller; (ii) the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller; (iii) the conclusion of a contract between the data controller and a person other than the data subject which (A) is entered into at the request of the data subject; or (B) is in the interest of the data subject; (iv) the performance of a contract described in subparagraph (iii); (v) reasons of substantial public interest; (vi) the purpose of, or in connection with, any legal proceedings including prospective legal proceedings; (vii) the purpose of obtaining legal advice; (viii) the purposes of establishing, exercising or defending legal rights; or (ix) the protection of the vital interests of the data subject;	

Title	Types of Data Covered	Selected Rules in Barbados on Cross-Border Data Transfers or Data Localization	Sources
		(c) the transfer of personal data is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data is or may be disclosed after the transfer; (d) the transfer of personal data is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects; or (e) the transfer of personal data has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects. **Non-compliance** **27.** A person who contravenes sections 22, 23 or 24 is guilty of an offence and is liable on summary conviction to a fine of $500 000 or to imprisonment for 3 years or to both. **Substantial public interest** **28.**(1) The Minister may by order specify the (a) circumstances in which a transfer of the personal data of data subjects outside of Barbados is to be considered to be necessary for reasons of substantial public interest; and (b) circumstances in which a transfer of the personal data of data subjects outside of Barbados, which is not required by or under an enactment, is not to be considered necessary for reasons of substantial public interest. (2) An order made pursuant to subsection (1) shall be subject to negative resolution.	

Belgium

Title	Types of Data Covered	Selected Rules in Belgium on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Benin

Title	Types of Data Covered	Selected Rules in Benin on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The data protection regime in Benin is governed by two pieces of legislations namely the Law No. 2017-20 of April 20, 2018 on the digital code and the Law No. 2009-09 of May 22, 2009 dealing with the Protection of Personally Identifiable Information. A personal data processor may transfer data to a foreign country if the receiving country ensures an adequate level of protection for the privacy and human rights and freedoms of the persons concerned. The level of protection will be assessed according to: • the data protection laws of the recipient country; • the safety measures; and • the processing characteristics (end, duration, nature, origin, destination of processed data). It is worth noting that a country may not provide sufficient data protection, but if a recipient country is not deemed 'safe' in protecting data, but a data transfer is followed by protective measures such as contractual clauses or internal rules, assent could be provided by the APDP (The Beninese data protection authority). For instance, some data, such as biometric data, health data, data related to serious infringements, and data regarding crime, will be considered as involving specific risks for human rights and freedom of individuals' data. These data will need to be approved under Article 41 of the Law on the Protection of Personally Identifiable Information.	Transfer in Benin - DLA Piper Global Data Protection Laws of the World (dlapiperdataprotection.com)
Loi n° 2017-20 portant code du numérique en République du Bénin	Personal	Not excerpted or summarized due to lack of translation.	Benin-Loi-2017-20-Portant-code-du-numerique-en-Republique-du-Benin.pdf (afapdp.org)
Law No. 2009-09 of May 22,2009 - Dealing with the protection of Personally Identifiable Information (PII)	Personal	Excerpt **CHAPTER IV** - COMMISSION IN CHARGED OF THE PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION AND PROCESSINGS VERIFICATION/CONTROL **Article 9:** The responsible of a personally identifiable information can only transfer the data to a Foreign Government if the subject country warranties sufficient degre of privacy, liberty and unalienable rights protection of the subject individuals that such data identify. The degre of protection warrantied by a foreign country is evaluated based on the protection measures enforced in the very foreign Country, the security measures enforced in it, clear definition of the processing details such as its motivation, period/length as well as the nature, the origin and the destination of the processed data. **Section 43**: The processings indicated below may only be carried out upon the authorization and prior control of the Commission because of the particular risks for the rights and privacies or when the content and their motives are susceptible to interfere with the privacy of the indivudual involved in the processing of personally identifiable information: a) The Processings that include a national identification number as well as all nationwide processings taking census of the entire population or part of it; b) The processings that include sufficient biometric data/information for the tracking of individuals' identities; c) The processings that include health related information/data of individuals or their situation/location; d) The processings that include information/data related to the infrengements and condemnations; e) The processings related the homeland security, the defence or the public safety and the ones that deal with the prevention, researching, the verification or the tracking of penal infrengements or the execution of penal condemnations; f) The processings that aim at the interconnexion of files corresponding to different interests;	https://apdp.bj/wp-content/uploads/2016/08/Loi-No-2009-du-22Mai-2009-Version-Anglaise.pdf

Title	Types of Data Covered	Selected Rules in Benin on Cross-Border Data Transfers or Data Localization	Sources
		g) Processings that can deny individuals the favour/benefit of a right, a performance or a contract; h) Processings that allow for transfers of personal data/information to other foreign countries when the processing warrants sufficient degre of privacy protection as well as liberties and unalienable human rights, also for contractual terms or internal rules that it is subject to.	

Bhutan

Title	Types of Data Covered	Selected Rules in Bhutan on Cross-Border Data Transfers or Data Localization	Sources
Information, Communications and Media Act of Bhutan 2018	Personal	No provisions relating to international transfer or processing of personal data	https://www.dit.gov.bt/sites/default/files/attachments/ICM%20Act%202018.pdf

Bolivia

Title	Types of Data Covered	Selected Rules in Bolivia on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Under the Bill of Personal Data Protection, the person responsible within the Personal Data Protection Authority may only process personal data when the owner grants his consent for one or more specific purposes, when necessary for the fulfilment of a court order, for the defence or recognition of the rights of the holder/owner before a public authority, to protect the vital interests of the holder/owner or of another natural person; among other legitimate and informed reasons. Nothing in the Bill of Personal Data Protection is established concerning transfer.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=BO
Ley general de Telecomunicaciones, Tecnologías de Información y Comunicación – Ley 167 de 08 agosto de 2011 (in Spanish)	Personal	Not excerpted or summarized due to lack of translation.	https://www.wipo.int/edocs/lexdocs/laws/es/bo/bo052es.pdf

Bosnia and Herzegovina

Title	Types of Data Covered	Selected Rules in Bosnia and Herzegovina on Cross-Border Data Transfers or Data Localization	Sources
Law on Protection of Personal Data („Official Gazette of Bosnia and Herzegovina“ 49/06)	Personal	Excerpt **Article 18** - Data Transfer Abroad (1) Personal data shall not be transferred from Bosnia and Herzegovina to a controller or processor abroad regardless of data medium or the manner of transfer unless the requirements specified in Article 4 hereof have not been fulfilled in the receiving country and provided that that the foreign controller shall comply with equal data protection principles for all data. (2) Exceptionally, the personal data may be transferred abroad if the data subject has consented to the transfer, where it is required for the purpose of fulfilling the contract or legal claim and when it is required for the protection of public interest. **Article 4** - Principles of Personal Data Processing The controller shall be required to: a) process personal data fairly and lawfully b) process personal data collected for special, explicit and lawful purposes in no manner contrary to the specified purpose; c) process personal data only to the extent and scope necessary for the fulfilment of the specified purpose; d) process only authentic and accurate personal data, and update such data when necessary; e) erase or correct personal data which are incorrect and incomplete, given the purpose for which the data are collected or further processed; f) process personal data only within the period of time necessary for the fulfilment of the purpose of their processing. g) keep personal data in the format that allows identification of the data subject for not longer than required for the purpose for which the data are collected or further processed; h) ensure that personal data that were obtained for various purposes are not combined or merged.	http://www.azlp.ba/propisi/default.aspx?id=8&langTag=en-US&template_id=149&pageIndex=1

Botswana

Title	Types of Data Covered	Selected Rules in Botswana on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The Data Protection Act – Act No. 32 of 2018, ("the DPA") is an Act which was assented to by Parliament on the 3rd August 2018 and came into effect on the 15th of October 2021. The DPA regulates the protection of personal data and ensure that the privacy of individuals in relation to their personal data is maintained. The transfer of personal data from Botswana to another country is prohibited save for transborder transfers to countries that have been designated by the Minister through an Order published in the Government Gazette. Transborder transfers of personal data require prior authorisation to be granted by the Commissioner so as to assess and ensure that adequate levels of protection are provided by the country receiving the personal data. The assessment is in light of all the circumstances surrounding the data transfer operation and particular consideration is given to: • the nature of the data; • the purpose and duration of the proposed processing operation; • the country of origin and the country of final destination; • the rule of law, both general and sectoral, in force in the third country in question; and • the professional rules and security safeguards which are complied with in that country. Notwithstanding the above, transborder transfers to countries which do not offer an adequate level of protection are allowed where the data subject consents to the proposed transfer or, where the transfer is: • necessary for the performance of a contract between the data subject and the data controller, or the implementation of pre contractual measures taken in response to the data subject's request; • necessary for the performance or conclusion of a contract in the interests of the data subject between the data controller and a third party; • necessary for the public interest, or for the establishment, exercise or defence of a legal claim; • necessary to protect the vital interests of the data subject; or • made from a register that is intended to provide the public with information and is open to public inspection. Regardless of the above mentioned restrictions, transborder flow of personal data to a country without adequate levels of protection may be authorised where the data controller provides adequate safeguards which may be by means of appropriate contractual provisions, with respect to the protection of the privacy and fundamental rights and freedoms of individuals.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=BW
Data Protection Act, 2018 (No. 32 of 2018)	Personal	Excerpt PART VIII – Miscellaneous Provisions **Transborder flow of personal data** **48.** (1) The transfer of personal data from Botswana to another country is prohibited. (2) Notwithstanding the generality under subsection (1), the Minister may, by Order published in the Gazette, designate the transfer of personal data to any country listed in such Order. **Transfer of personal data to third country**	https://www.bocra.org.bw/sites/default/files/documents/DataProtectionAct.pdf https://www.botswanalaws.com/acts-on-notice/data-protection

Title	Types of Data Covered	Selected Rules in Botswana on Cross-Border Data Transfers or Data Localization	Sources
		49. (1) Without prejudice to section 48, and subject to the provisions of this Act, the transfer of personal data that is undergoing processing or intended processing, to a third country may only take place if the third country to which the data is transferred ensures an adequate level of protection. (2) The adequacy of the level of protection of data by a third country referred to under subsection (1) shall be assessed by the Commissioner in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations, and particular consideration shall be given to (a) the nature of the data; (b) the purpose and duration of the proposed processing operation; (c) the country of origin and country of final destination; (d) the rule of law, both general and sectoral, in force in the third country in question; and (e) the professional rules and security safeguards which are complied with in that country. (3) The Commissioner shall decide whether a third country ensures adequate security safeguards. (4) The transfer of personal data to a third country that does not ensure adequate security safeguards is prohibited. (5) Notwithstanding subsection (4), a transfer of personal data to a third country that does not ensure adequate security safeguards may be effected by the data controller if the data subject has given his or her consent to the proposed transfer or if the transfer — (a) is necessary for the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken in response to the data subject's request; (b) is necessary for the performance or conclusion of a contract concluded or to be concluded in the interests of the data subject between the data controller and a third party; (c) is necessary or legally required for the public interest, or for the establishment, exercise or defence of a legal claim; (d) is necessary in order to protect the vital interests of the data subject; or (e) is made from a register that according to any law, is intended to provide information to the public and which is open for public inspection, (6) Notwithstanding subsection (1), the Commissioner may authorise a transfer or a set of transfers of personal data to a third country that does not ensure an adequate level of security safeguards within the meaning of subsection (2): Provided that the data controller provides adequate safeguards, which may result by means of appropriate contractual provisions, with respect to the protection of the privacy and fundamental rights and freedoms of individuals and with respect to their exercise.	https://www.dataguidance.com/notes/botswana-data-protection-overview

Brazil

Title	Types of Data Covered	Selected Rules in Brazil on Cross-Border Data Transfers or Data Localization	Sources

Summary	Personal	The transfer of personal data to other jurisdictions is allowed only subject to compliance with the requirements of the LGPD. Prior specific and informed consent is needed for such transfer, unless:
		
		• The transfer is to countries or international organizations with an adequate level of protection of personal data
		• There are adequate guarantees of compliance with the principles and rights of data subject provided by LGPD, in the form of
		  o Specific contractual clauses for a given transfer
		  o Standard contractual clauses
		  o Global corporate norms, or
		  o Regularly issued stamps, certificates and codes of conduct
		• The transfer is necessary for international legal cooperation between public intelligence, investigative and prosecutorial agencies
		• The transfer is necessary to protect the life or physical safety of the data subject or a third party
		• The ANPD has provided authorization
		• The transfer is subject to a commitment undertaken through international cooperation
		• The transfer is necessary for the execution of a public policy or legal attribution of public service
		• The transfer is necessary for compliance with a legal or regulatory obligation, execution of a contract or preliminary procedures related to a contract, or the regular exercise of rights in judicial, administrative or arbitration procedures
			DLA Piper, *Data Protection Laws of the World*, at: https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all

General Law on the Protection of Personal Data (LGPD). (Wording given by Law No. 13,853, 2019)	Personal	Excerpt CHAPTER I - PRELIMINARY PROVISIONS **Art. 4** This Law does not apply to the processing of personal data: I - performed by a natural person for exclusively private and non-economic purposes; II - carried out for purposes exclusively: a) journalistic and artistic; or b) academics, applying to this hypothesis the arts. 7th and 11th of this Law; III - carried out for the exclusive purposes of: a) public security; b) national defense; c) state security; or d) investigation and prosecution of criminal offences; or IV - from outside the national territory and that are not the object of communication, shared use of data with Brazilian agents or subject to international data transfer with a country other than the source, provided that the country of provenance provides a degree of protection of personal data appropriate to the provisions of this Law. § 1 - The processing of personal data provided for in item III shall be governed by specific legislation, which shall provide for measures proportionate and strictly necessary to meet the public interest, subject to due process, the general principles of protection and the rights of the holder provided for in this Law. § 2 - The processing of the data referred to in item III of the caput of this article by a person under private law, except in proceedings under the protection of a legal entity under public law, which shall be subject to specific information to the national authority and which shall observe the limitation imposed in § 4 of this article, is limited.	http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

Title	Types of Data Covered	Selected Rules in Brazil on Cross-Border Data Transfers or Data Localization	Sources
		§ 3 - The national authority shall issue technical opinions or recommendations regarding the exceptions provided for in item III of the caput of this article and shall request responsible authorities to report on the protection of personal data. § 4 - In no case may all personal data in the database of the caput of this article be treated by a person under private law, except for the person with capital wholly constituted by the public authorities. (Wording given by Law No. 13,853, 2019) Validity CHAPTER V - OF INTERNATIONAL DATA TRANSFER **Art. 33.** International transfer of personal data is only permitted in the following cases: I - for countries or international organizations that provide the degree of protection of personal data appropriate to the provisions of this Law; II - when the controller offers and proves guarantees of compliance with the principles, rights of the holder and the data protection regime provided for in this Law, in the form of: (a) specific contractual clauses for a given transfer; b) standard contractual clauses; c) global corporate standards; (d) regularly issued stamps, certificates and codes of conduct; III - where the transfer is necessary for international legal cooperation between public intelligence, investigative and pursuit bodies in accordance with the instruments of international law; IV - where the transfer is necessary for the protection of the life or physical safety of the holder or third party; V - when the national authority authorises the transfer; VI - when the transfer results in a commitment made in an international cooperation agreement; VII - when the transfer is necessary for the execution of public policy or legal attribution of the public service, being given publicity in accordance with item I of the caput of art. 23 of this Law; VIII - when the holder has provided his specific consent and highlighted the transfer, with prior information on the international character of the operation, clearly distinguishing it from other purposes; or IX - when necessary to meet the hypotheses provided for in items II, V and VI of art. 7 of this Law. Single paragraph. For the purposes of item I of this article, legal entities of public law referred to in the sole paragraph of Article 1 of Law No. 12,527 of November 18, 2011 (Law on Access to Information) within the scope of their legal powers, and responsible, within the scope of their activities, may request the national authority to assess the level of protection of personal data conferred by a country or international body. **Art. 34.** The level of data protection of the foreign country or the international body mentioned in article 33 of art. 33's caput i of this Law shall be assessed by the national authority, which shall take into account: I - the general and sectoral rules of legislation in force in the country of destination or in the international body; II - the nature of the data; III - compliance with the general principles of protection of personal data and rights of holders provided for in this Law; IV - the adoption of security measures provided for in the Regulation; V - the existence of judicial and institutional guarantees for respect for the rights of protection of personal data; and VI - other specific circumstances relating to the transfer.	
Guidelines on Government Procurement of Cloud Services, 2018	All	The Guidelines on Government Procurement of Cloud Services were issued in late 2018 and include server and data localization requirements that negatively impact the procurement of cloud computing services by all federal agencies. The subsequently issued final Guidelines also included these localization requirements	

Bulgaria

Title	Types of Data Covered	Selected Rules in Bulgaria on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Burkina Faso

Title	Types of Data Covered	Selected Rules in Burkina Faso on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The data protection regime in Burkina Faso is governed by the following laws and regulations: • Law No. 001-2021 of March 30, 2021 on the protection of persons with regard to the processing of personal data. • Law 010-2004/AN on the protection of personal data. • Decree No. 2007-283/PRES/PM/MPDH of 18 May 2007 regarding the organisation and functioning of the Commission de l'Informatique et des Libertés; • Decree No. 2007-757/PRES/PM/MPDH/MEF appointing the members of the Commission de l'Informatique et des Libertés ; and • Order No. 2008/001/CIL fixing the internal regulations of the Commission de l'Informatique et des Libertés. Burkina Faso's data protection authority is the Commission de l'Informatique et des Libertés ('**CIL**'). Burkina Faso has also adopted on 22 November 2013 the Marrakech resolution issued by the French-speaking association of data protection authorities relating to the procedure for the supervision of personal data transfers of personal data in the French-speaking world by means of binding corporate rules. The provisions of the Law pertaining to international transfers are broadly drafted. According to said provisions, international transfers cannot be made without the respect of the following conditions: • To request the authorisation of the CNIL; • To sign with the contracting party, a data confidentiality clause and a data reversibility clause in order to facilitate the complete migration of the data at the end of the contract; • Implement technical and organisational security measures. Additionally, the transfer can only be made to a foreign country or an international organisation if the beneficiary country or international organisation ensures an adequate level of protection equal to the one ensured in Burkina Faso (Article 42 of the law). As a signatory to the Marrakech Resolution of 22 November 2013, Burkina Faso recognizes the application of the French-speaking RCE, which consist in a code of conduct by which a group of companies defines its internal policy on the transfer of personal data. The RCE are based and designed on the model of the European Commission's binding corporate rules ('**BCR**'). In practice, the RCE mechanism concerns the authorities of the AFAPDP member countries that have adopted the cooperation protocol and the resolution on the framework for data transfers in the French-speaking area. These concerns at least the following 13 countries: Albania, Andorra, Belgium, Benin, Burkina Faso, France, Gabon, Luxembourg, Mauritius, Morocco, Senegal, Switzerland and Tunisia. The RCE cover intra-group transfers of personal data carried out by a company established in an AFAPDP member country, to other companies of the group, whether the latter are located in an AFAPDP member country or not.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=BF
Loi n° 010-2004/AN Portant Protection des Données à Caractère Personnel (in French)	Personal	Not excerpted or summarized due to lack of translation.	https://www.afapdp.org/wp-content/uploads/2012/01/Burkina-Faso-Loi-portant-protection-des-donn%c3%a9es-%c3%a0-caract%c3%a8re-personnel-20042.pdf

Title	Types of Data Covered	Selected Rules in Burkina Faso on Cross-Border Data Transfers or Data Localization	Sources

Title	Types of Data Covered	Selected Rules in Canada on Cross-Border Data Transfers or Data Localization	Sources
Jurisdiction Summary	Personal	**Summary:** When an organization transfers personal information to a third party service provider (ie, who acts on behalf of the transferring organization -- although Canadian legislation does not use these terms, the transferring organization would be the "controller" in GDPR parlance, and the service provider would be a "processor"), the transferring organization remains accountable for the protection of that personal information and ensuring compliance with the applicable legislation, using contractual or other means. In particular, the transferring organization is responsible for ensuring (again, using contractual or other means) that the third party service provider appropriately safeguards the data, and would also be required under the notice and openness/transparency provisions to reference the use of third party service providers in and outside of Canada in their privacy policies and procedures. These concepts apply whether the party receiving the personal information is inside or outside Canada. Transferring personal information outside of Canada for storage or processing is generally permitted so long as the requirements discussed above are addressed, and the transferring party notifies individuals that their information may be transferred outside of Canada and may be subject to access by foreign governments, courts, law enforcement or regulatory agencies. This notice is typically provided through the transferring party's privacy policies. With respect to the use of foreign service providers, PIPA Alberta specifically requires a transferring organization to include the following information in its privacy policies and procedures: • The countries outside Canada in which the collection, use, disclosure or storage is occurring or may occur, and • The purposes for which the third party service provider outside Canada has been authorized to collect, use or disclose personal information for or on behalf of the organization Under PIPA Alberta, specific notice must also be provided at the time of collection or transfer of the personal information and must specify: • The way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada, and • The name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organization. In addition, under the Quebec Privacy Act, an organization must take reasonable steps to ensure that personal information transferred to service providers outside Quebec will not be used for other purposes and will not be communicated to third parties without consent (except under certain exceptions prescribed in the Act). The Quebec Privacy Act also specifically provides that the organization must refuse to transfer personal information outside Quebec where it does not believe that the information will receive such protection. Starting September 22, 2023, the Quebec Privacy Act, as modified by Bill 64, will require all organizations, before transferring personal information outside of the province of Quebec, to conduct data privacy assessments and enact appropriate contractual safeguards to ensure that the information will benefit from adequate protection in the jurisdiction of transfer. These assessments must take into account the sensitivity of the information, the purposes, the level of protection (contractual or otherwise) and the applicable privacy regime of the jurisdiction of transfer. Quebec has decided not to implement a system of adequacy decisions, and therefore assessments will likely be required prior to any cross-jurisdiction transfer. Source: DLA Piper	
Personal Information Protection and Electronic Documents Act (Current to February 23, 2022; Last amended on	Personal	Excerpt **Disclosure of information to foreign state** **23.1** (1) Subject to subsection (3), the Commissioner may, in accordance with any procedure established under paragraph (4)(b), disclose information referred to in subsection (2) that has come to the Commissioner's knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Part to any person or body who, under the legislation of a foreign state, has (a) functions and duties similar to those of the Commissioner with respect to the protection of personal information; or	https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf

Title	Types of Data Covered	Selected Rules in Canada on Cross-Border Data Transfers or Data Localization	Sources
June 21, 2019)		(b) responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of this Part. Information that can be shared (2) The information that the Commissioner is authorized to disclose under subsection (1) is information that the Commissioner believes (a) would be relevant to an ongoing or potential investigation or proceeding in respect of a contravention of the laws of a foreign state that address conduct that is substantially similar to conduct that would be in contravention of this Part; or (b) is necessary to disclose in order to obtain from the person or body information that may be useful to an ongoing or potential investigation or audit under this Part. Written arrangements (3) The Commissioner may only disclose information to the person or body referred to in subsection (1) if the Commissioner has entered into a written arrangement with that person or body that (a) limits the information to be disclosed to that which is necessary for the purpose set out in paragraph (2)(a) or (b); (b) restricts the use of the information to the purpose for which it was originally shared; and (c) stipulates that the information be treated in a confidential manner and not be further disclosed without the express consent of the Commissioner. Arrangements (4) The Commissioner may enter into arrangements with one or more persons or bodies referred to in subsection(1) in order to (a) provide for cooperation with respect to the enforcement of laws protecting personal information, including the sharing of information referred to in subsection (2) and the provision of mechanisms for the handling of any complaint in which they are mutually interested; (b) establish procedures for sharing information referred to in subsection (2); (c) develop recommendations, resolutions, rules, standards or other instruments with respect to the protection of personal information; (d) undertake and publish research related to the protection of personal information; (e) share knowledge and expertise by different means, including through staff exchanges; or (f) identify issues of mutual interest and determine priorities pertaining to the protection of personal information.	

Cape Verde

Title	Types of Data Covered	Selected Rules in Cape Verde on Cross-Border Data Transfers or Data Localization	Sources
Lei n° 133/V/2001 of 22 January 2001 (in Portuguese)	Personal	Not excerpted or summarized due to lack of translation.	https://www.afapdp.org/wp-content/uploads/2012/01/Cap-vert-Lei-n%c2%b0133-V-2001-do-22-janeiro-20011.pdf

Chad

Title	Types of Data Covered	Selected Rules in Chad on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The data protection regime in Chad is mainly governed by the following laws and regulations: • Act No. 007/PR/2015 of February 10, 2015, on Personal Data protection ('**The Act**') • Decree No. 075/PR/2019 of January 21, 2019 implementing the provisions of application of the Act N°007/PR/2015 of February 10, 2015 on the protection of personal data • Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification • Ordinance No. 002/PR/2019 amending Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification • Ordinance No. 009/PCMT/2022 amending Act No. 006/PR/2015 on the creation of the National Agency for Computer Security and Electronic Certification • Act No. 009/PR/2015 on the cybersecurity and the fight against the cybercrime • Ordinance No. 008/PCMT/20022 on the Cybersecurity in the Republic of Chad • Act No. 008/PR/2015 on electronic transactions In light of Article 29 of the Act, the data controller cannot transfer personal data to another foreign country non-member of the CEMAC/CEAC unless that country provides a sufficient level of protection for the privacy, fundamental rights, and freedoms of individuals. Moreover, prior to any transfer of personal data abroad, the data controller must first inform the regulatory authority, ANSICE. CEMAC is the French acronym of Economic and Monetary Community of Central Africa. CEEAC is the French acronym of the Economic Community of Central Africa States. A transfer to a non CEMAC/CEEAC country not offering a sufficient level of protection is possible if: • the Data Subject agrees to the transfer; • the transfer protects the life of the Data Subjects/Holders; • the transfer Protect the public interest; • the transfer is necessary to the performance of an agreement between the Data Subject and the Data Processor or take precontractual measures upon the request of the Data Subject; • If the transfer intervenes from a public register which, according to law and regulations, is focused on the public information and open to the public consultation. The ANSICE may allow the Data controller to transfer data to a foreign country non-member of CEMAC/CEEAC if the Data controller provides sufficient protection for the Data Subject's private life, liberties, and fundamental rights. (Articles 30-33 of the Act)	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=TD
Law 007/PR/2015 on the Protection of Personal Data (in French and Arabic)	Personal	Not excerpted or summarized due to lack of translation.	https://arcep.td/sites/default/files/Loi-N%C2%B007-PR-2015.pdf

Chile

Title	Types of Data Covered	Selected Rules in Chile on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Law 19,628/1999 'On the protection of private life', commonly referred to as 'Personal Data Protection Law' (hereinafter, the 'PDPL') generally defines and regulates the processing of personal data in public and private databases and is thus the primary body of rules on the processing of personal data not governed by sectoral provisions. Generally, the PDPL stipulates that personal data may only be processed if the processing is (i) permitted by law (*eg*, labor law, health care law, etc.) or (ii) based on the data subject's prior informed, written consent. There are only a few narrow exceptions to this principle (*eg*, certain publicly accessible data, or purely internal data processing for certain purposes). Transfer of personal data is considered a processing activity, so all of the aforementioned rules are applicable, including the requirement to rely on a legal basis (usually consent). The PDPL does not provide or require any special provisions for the international transfer of personal data.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=CL
Law 19.628 of 1999 – On the Protection of Privacy (PDPL)	Personal	Excerpt (translated version) **Article 5.-** The person responsible for the registry or bank of personal data may establish an automated transmission procedure, provided that the rights of the holders are safeguarded and the transmission is related to the tasks and purposes of the participating organizations. Faced with a request for personal data through an electronic network, it must be recorded: (a) The individualization of the applicant; (b) The reason for and purpose of the request, and (c) The type of data being transmitted. The admissibility of the request will be evaluated by the person in charge of the database that receives it, but the responsibility for said request will be of the one who makes it. The recipient may only use the personal data for the purposes for which the transmission was motivated. This Article shall not apply in the case of personal data accessible to the general public. This provision also does not apply when personal data is transmitted to international organizations in compliance with the provisions of current treaties and conventions.	https://www.bcn.cl/leychile/navegar?idNorma=141599
Law 20,575/2012 establishing the 'purpose principle' for the processing of personal data of an economic, financial, banking or commercial nature		Does this contain localization requirements? This law establishes several rules that apply to the processing of personal data referring to financial, economic, banking or commercial information, such as: Providers of economic, financial, banking or commercial databases must have a system for recording the name of any person requesting database information, the reason, date and time of the request and the person responsible for delivering or transferring the information. Data subjects have the right to request access to their commercial information every four months and free of charge.	
Bill regulating the protection and processing of personal data and creating the Agency for the Protection of Personal Data (Bulletin 11,144-07,	Personal	This draft law aims to modernize the PDPL and adapt it to international standards. The most important stipulations are: • the introduction of further legal bases for the processing of personal data in addition to consent (such as performance of a contract and legitimate interest), and additional requirements for processing sensitive data, depending on the category of data concerned. • various basic principles, such as lawfulness, purpose limitation, proportionality, data quality, accountability, security, transparency and information, and confidentiality. • regulations on international data transfers. • information requirements. • special obligations when using data processors.	

Title	Types of Data Covered	Selected Rules in Chile on Cross-Border Data Transfers or Data Localization	Sources
consolidated with Bulletin 11,092-07)		• provisions on data protection by design and default and security measures. • reporting obligations in the event of data breaches. • introduction of the right to portability. • the creation of a data protection authority with the competence to impose administrative fines. The bill has been under debate for some time but is currently still in the first constitutional stage in the senate. There is currently no indication when it may pass.	

China

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
Summary	Various	There is not a single comprehensive data protection law in the People's Republic of China (PRC). Instead, rules relating to personal information protection and data security are part of a complex framework and are found across various laws and regulations. That said, the three main pillars of the personal information protection framework in the PRC are the Personal Information Protection Law (PIPL), the Cybersecurity Law (CSL), and the Data Security Law (DSL). On June 1, 2017, the CSL came into effect and became the first national-level law to address cybersecurity and data privacy protection. The DSL came into force on September 1, 2021, and focuses on data security across a broad category of data (not just personal information). Most significantly, the PIPL came into effect on November 1, 2021. The PIPL is the first comprehensive, national-level personal information protection law in the PRC. The PIPL does not replace – but instead enhances and clarifies - earlier personal information laws and regulations. In addition to the PIPL, CSL and DSL, the following form the backbone of general personal information protection framework currently in the PRC: • The Decision on Strengthening Online Information Protection, effective from December 28, 2012 (Decision); • National Standard of Information Security Technology – Guideline for Personal Information Protection within Information System for Public and Commercial Services, effective from February 1, 2013; • The Draft Regulation of Network Data Security Management, published for consultation in November, 2021; and • The Draft Measures for Security Assessment of Cross-border Data Transfer, published for consultation in October, 2021. In the past five years, there has also been an abundance of implementing regulations and guidelines (herein referred to as Guidelines) proposed, issued or revised to flesh out the essentials and concepts introduced under the personal information protection framework. These include, non-exhaustively: • National Standard of Information Security Technology – Personal Information Security Specification (PIS Specification), as amended and effective from October 1, 2020; • Guidelines on Internet Personal Information Security Protection, effective from April 19, 2019; and • National Standard of Information Security Technology – Guidelines on Personal Information Security Impact Assessment, effective from June 1, 2021. If a data controller wishes to share, disclose or otherwise transfer an individual's personal information to a third party (including group companies), the data controller must: • inform the data subject of the purposes of the sharing, disclosure or transfer of the personal information and the types of data recipient, and obtain prior express consent from the data subject; • perform a personal information impact assessment (PIIA), and take effective measures to protect the data subjects according to the assessment results (e.g. putting in place a data transfer agreement or similar contractual protections) (see Collection & Processing); • record accurately and keep the information in relation to the sharing, disclosure or transfer of the personal information, including the date, scale, purpose and basic information of the data recipient of the sharing or assigning; • ensure personal information is only transferred where required for processing purposes; • not share or transfer any personal biometric information or other types of particularly sensitive personal information where prohibited under relevant laws or regulations; and • ensure contractual measures are entered into to require the data processor to comply or assist the data controller in complying with obligations under data protection laws.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=CN

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
		The PIPL provided helpful clarification (after years of uncertainty) on the issue of cross-border data transfers and data localization in the PRC. In short, most personal information can be transferred or accessed outside of the PRC providing the following compliance steps are taken: • one of the following criteria is fulfilled: o the organisation has passed a CAC security evaluation; o the organisation has obtained certification from a CAC-accredited agency; o the organisation has put in place CAC standard contractual clauses (not yet published) with the data recipient – likely to be most relied upon in practice; or o for compliance with laws and regulations or other requirements imposed by the CAC; • the data controller has adopted necessary measures to ensure the data recipient's data processing activities comply with standards comparable to those set out in the PIPL. In practice this means initial due diligence, sufficient contractual protections and ongoing monitoring etc.; • notice and separate, explicit consent has been given/obtained (see above) from the data subject (see Collection & Processing); and • a PIIA has been conducted. Certain personal information (and non-personal data) must still remain in (and cannot be accessed outside of) the PRC. This includes: • personal information processed by critical information infrastructure operators (CIIOs), unless a CAC-conducted security assessment has been completed; • personal information processed by data controllers above a threshold/volume to be identified by the CAC (not yet finalised), unless a CAC-conducted security assessment has been completed; • certain data under industry-specific regulations (such as in the financial services sector and genetic health data); and • certain restricted data categories (such as "state secrets", some "important data", geolocation and online mapping data etc.). Lingering uncertainty remains about the need for a CAC-conducted security assessment in certain situations. The Draft Guidelines on Overseas Transfer (published in November 2021) proposes a host of scenarios where this may be the case, including: personal information processed in the context of certain listing/corporate/restructuring activities; and processing of large volumes of personal information and/or sensitive personal information. The Draft Network Data Security Management Regulation also proposes introducing annual data overseas transfer security report to the CAC as well as other record keeping requirements. As such, organizations should keep developments under review. Finally, according to the PIPL: • a new publicly-available entity list may be published, listings foreign organisations to whom local PRC organisations may not transfer personal information, where such transfer may harm national security or public interest; • data controllers must not provide personal information stored within China to overseas legal or enforcement authorities unless approval is obtained from a designated Chinese authority. It remains unclear whether this extends to, say, requests from overseas industry regulators; and • the PIPL clarifies that Chinese authorities may provide personal information stored within China to overseas legal or enforcement authorities upon request, if and to the extent that there are international treaties or regulations in place to maintain fairness and for mutual benefit.	
Cybersecurity Law of China (Passed November 6, 2016. Effective June 1, 2017.)	Critical information, personal data	Excerpt: Article 37: Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions.	Cybersecurity Law of China (DigiChina translation) (Data Guidance translation) Other sources: KPMG

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
		Article 38: At least once a year, critical information infrastructure operators shall conduct an inspection and assessment of their networks' security and risks that might exist, either on their own or through retaining a cybersecurity services organization; CII operators should submit a cybersecurity report on the circumstances of the inspection and assessment as well as improvement measures, to be sent to the relevant department responsible for critical information infrastructure security protection efforts. Article 50: State cybersecurity and informatization departments and relevant departments will perform network information security supervision and management responsibilities in accordance with law; and where they discover the publication or transmission of information which is prohibited by laws or administrative regulations, shall request that network operators stop transmission, employ disposition measures such as deletion, and store relevant records; for information described above that comes from outside the mainland People's Republic of China, they shall notify the relevant organization to adopt technical measures and other necessary measures to block transmission. Article 66: Where critical information infrastructure operators violate Article 37 of this Law by storing network data outside the mainland territory, or provide network data to those outside of the mainland territory, the relevant competent department: shall order corrective measures, provide warning, confiscate unlawful gains, and levy fines between RMB 50,000 and 500,000; and may order a temporary suspension of operations, a suspension of business for corrective measures, closing down of websites, revocation of relevant operations permits, or cancellation of business licenses. Persons who are directly in charge and other directly responsible personnel shall be fined between RMB 10,000 and 100,000.	
Personal Information Protection Law (Passed at the 30th meeting of the Standing Committee of the 13th NPC on August 20, 2021. Effective November 1, 2021)	Personal	Summary: The **Personal Information Protection Law ("PIPL")** took effect on November 1, 2021. The PIPL raises the following concerns: (1) data localization requirements for "personal information" (PIPL Art. 40) and highly restrictive data transfer provisions for "personal information" (PIPL Arts. 38-40); (2) lack of definition or broad scope for key concepts that implicate data localization requirements and data transfer restrictions, including what constitutes a "justified need," or a "large volume [of data]" (PIPL Art 40); (3) mandates for data assessments requiring governmental notification and/or approval in conjunction with the data localization and data transfer provisions noted above (PIPL Art. 38(1), 40); (4) proposed data transfer "standard contracts" that, while encouraging, may not be interoperable with standard contractual clauses under the EU General Data Protection Regulation (GDPR) or other established personal data protection frameworks (PIPL, Art. 38(3)); (5) the absence from the PIPL of other internationally recognized data transfer mechanisms, such as intra-corporate binding rules, trustmarks and regional certifications (PIPL, Art. 38); and (6) pre-transfer requirements for separate consent from individuals, even where another legal basis for transfer (such as contractual clauses) has been established. (PIPL, Art. 39). (7) the ability for Chinese authorities to adopt retaliatory measures against overseas organization or individuals who have infringed upon the personal information rights and interests of any citizen of China, or endangered the national security or public interests of China (PIPL, Art. 42-43) Excerpt: Chapter III Rules for the Cross-Border Provision of Personal Information **Article 38** Where a personal information handler does need to provide personal information to a recipient outside the territory of the People's Republic of China for business or other reasons, it shall meet any of the following conditions: (1) Having passed the security assessment conducted by the State cyberspace department in accordance with the provisions of Article 40 of this Law; (2) Having undergone the personal information protection certification conducted by a professional organization in accordance with the provisions of the State cyberspace department; (3) Having concluded a contract with the overseas recipient in accordance with the standard contract formulated by the State cyberspace department, defining the rights and obligations of both parties;	China, Personal Information Protection Law (China briefing translation; DigiChina translation)

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
		(4) Other conditions prescribed by laws, administrative regulations or the State cyberspace department. Where an international treaty or agreement concluded or joined by the People's Republic of China has provisions on the conditions for cross-border provision of personal information and more, the provisions may apply. Personal information handlers shall take necessary measures to ensure the personal information handling activities of overseas recipients meet the personal information protection standards specified in this Law. **Article 39** Where a personal information handler provides personal information to a recipient outside the territory of the People's Republic of China, it shall notify individuals of the name and contact information of the overseas recipient, the purpose and method of handling, the type of personal information and the manner in and the procedures by which the individuals exercise the rights under this Law to the overseas recipient, and obtain the individuals' separate consent. **Article 40** Operators of critical information infrastructure and personal information handlers who handle personal information whose volume has reached the threshold specified by the State cyberspace department shall ensure the personal information collected and generated within the territory of the People's Republic of China is stored in China. Where there is a justified need to provide to recipients overseas, the transfer shall pass the security assessment conducted by the State cyberspace department; where laws, administrative regulations and the State cyberspace department stipulate that a security assessment is not required, such provisions shall prevail. **Article 41** The competent authorities of the People's Republic of China, in accordance with relevant laws and international treaties and agreements concluded or joined by the People's Republic of China, or in adherence to the equality and reciprocity principles, handle the request of a foreign judicial or law enforcement agency for the provision of personal information stored within the territory of China. Without approval of the competent authorities of the People's Republic of China, personal information handlers shall not provide such personal information to foreign judicial or law enforcement agencies. **Article 42** Where an overseas organization or individual engages in personal information handling activities that infringe the personal information rights and interests of citizens of the People's Republic of China, or endanger the national security and public interests of the People's Republic of China, the State cyberspace department may include it/him in the list of entities/individuals subject to restrictions/ban concerning the provision of personal information, make it/him public, and take measures such as restricting or banning the provision of personal information to it/him. **Article 43** Where any country or region adopts discriminatory prohibitive, restrictive or other similar measures against the People's Republic of China in the protection of personal information, the People's Republic of China may take reciprocal measures against that country or region in the light of the actual situation.	
Data Security Law (Adopted at the 29th Meeting of the Standing Committee of the 13th NPC on June 10, 2021. Effective Sept. 1, 2021.)	Various	Summary: **The Data Security Law ("DSL")**, enacted on June 1, went into effect on September 1, 2021. The DSL: • Continues application of the 2017 Cybersecurity Rules on exportation of data by critical information infrastructure operators; • Requires the State Internet Information Department to draft rules for all "other data handlers" (i.e., not just CII operators) to restrict those other handlers' exportation of "important data"; • Applies to "[any person] handling important data"; • Requires the State to create a "categorical and hierarchical system for data protection" as well as "catalog of" for "important data" • Requires that the authorities assess the "importance" of data based on the following criteria: (1) Economic development; (2) Social development; (3) National security; (4) The public interest, or (5) Lawful rights and interests of citizens or organizations • Authorizes each region and department to set a "catalog of important data" within that region and in corresponding industries and sectors • Requires the State to create a "monitoring and early warning system" for important data, which will apparently help it prevent the exportation of "important data" Following the enactment of the Data Security Law (DSL), the Cyberspace Administration of China and sectoral regulators such as the Ministry of Industry and Information Technology are to develop draft guidelines to establish the requisite frameworks for data categorization and classification under the DSL The implementing rules and guidelines for DSL have been identified as a work item under the State Council's 2021 Legislative Work Plan.	Data Security Law. (DigiChina Translation). Other sources: Covington, CPO Magazine, DLA Piper, Federalist, Hogan, IAPP, JD Supra, Lexology, Ruibai, SCMP, WSJ.

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
		Excerpt: Chapter IV: Data Security Protection Obligations Article 27: The conduct of data handling activities shall be in compliance with the provisions of laws and administrative regulations, establishing and completing a data security management system for the entire workflow, organizing and conducting data security education and training, and adopting corresponding technical measures and other necessary measures to ensure data security. The conduct of data handling activities using the Internet or other such information networks shall perform the data security protection obligations described above on the basis of the cybersecurity Multi-Level Protection System. Important data handlers shall clearly designate persons responsible for data security, and management bodies to implement data security protection responsibilities. Article 28: The conduct of data handling activities and research and development of new data technologies shall be beneficial to promoting economic and social development, enhance the people's well-being, and conform to social morals and ethics. Article 29: The conduct of data handling activities shall strengthen risk monitoring, and when data security shortcomings, leaks, or other such risks are discovered, remedial measures shall be taken immediately; when data security incidents occur, methods to address them shall be taken immediately, promptly notifying users and reporting to relevant departments in charge as provided. Article 30: Those handling important data shall periodically conduct risk assessments of such data handling activities as provided and submit risk assessment reports to the relevant departments in charge. Risk assessment reports shall include the type and amount of important data being handled, the circumstances of the data handling activities, the data security risks faced and measures to address them, etc. Article 31: The provisions of the Cybersecurity Law of the PRC apply to the outbound security management[11] of important data collected or produced by critical information infrastructure operators operating within the mainland territory of the PRC; outbound security management measures for other data handlers collecting or producing important data within the mainland territory of the PRC are to be jointly formulated by the national cybersecurity and informatization department and relevant departments of the State Council. Article 32: Any organization or individual collecting data shall adopt lawful and proper methods and must not steal or otherwise obtain data through illegal methods. Where laws or administrative regulations have provisions on the purpose or scope of data collection and use, data shall be collected and used for the purpose and within the scope provided for by those laws and administrative regulations. Article 33: When institutions engaged in data transaction intermediary services provide services, they shall require the party providing the data to explain the source of the data, examine and verify the identities of both parties to the transactions, and retain verification and transaction records. Article 34: Where laws and administrative regulations provide that administrative permits shall be acquired for the provision of services related to data handling, service providers shall obtain permits in accordance with law. Article 35: Where public security authorities and national security authorities obtain data as necessary to safeguard national security or investigate crimes in accordance with law, they shall undergo strict approval procedures according to relevant State provisions and proceed in accordance with law, and relevant organizations and individuals shall cooperate. Article 36: The competent authorities of the PRC are to handle foreign justice or law enforcement institution requests for the provision of data, according to relevant laws and treaties or agreements concluded or participated in by the PRC, or in accordance with the principle of equality and reciprocity. Domestic organizations and individuals must not provide data stored within the mainland territory of the PRC to the justice or law enforcement institutions of foreign countries without the approval of the competent authorities of the PRC.	

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
		FN: “Outbound security management” (出境安全管理) refers to the security procedures and rules involved in transfer of data out of the mainland territory of the PRC.	
Outbound Data Transfer Security Assessment Measures (effective date, Sept. 1, 2022 with enforcement grace period until March 1, 2023)	Various	Summary: **The Outbound Data Transfer Security Assessment Measures** came into effect on September 1, 2022 with a six-month grace period for enforcement. Under these measures, all data processors are required to conduct self-assessments prior to cross-border data transfer. Additionally, data processors are required in enumerated cases to apply to CAC for a security assessment prior to cross-border data transfer. These cases involve: (1) Transfers of “important data”; (2) Cumulative transfers of personal information for >100,000 people, or sensitive personal info for >10,000 people; (3) Transfers by processors that have processed the personal information of >1 million people; (4) Transfers of personal information or important data generated/collected by Critical Information Infrastructure; and (5) Other circumstances in which CAC deems the security assessment to be necessary. Excerpt: Cyberspace Administration of China Article 1 These Measures are developed with a view to regulating the cross-border transfer of data, protecting the personal information rights and interests, safeguarding national security and public interests, and promoting the secure and free cross-border flow of data, in accordance with applicable laws including the Cybersecurity Law of the People’s Republic of China, the Data Security Law of the People’s Republic of China, and the Law of the People’s Republic of China on Personal Information Protection and related regulations. Article 2 Where a data handler is to provide abroad the critical data or personal information that is collected and generated by it during its operations within the territory of the People’s Republic of China, a security assessment of such transfer is governed by these Measures. Where it is otherwise provided for in laws or administrative regulations, such provisions shall prevail. Article 3 The security assessment of crossborder data transfer shall adhere to the principles of combining ex ante assessment with continuous supervision, and combining risk self-assessment with security assessment, to prevent security risks to cross-border data transfer and ensure a lawful, orderly and free flow of data. Article 4 Where a data handler is to provide data abroad under any of the following circumstances, it shall, through the local provincial-level cyberspace department, apply to the State cyberspace department for a security assessment over the cross-border transfer of data: (1) The data handler is to provide critical data abroad. (2) An operator of critical information infrastructure, or a personal information processor who processes personal information of one million people or more, is to provide personal information abroad; (3) The data handler having provided abroad the personal information of a cumulative total of 100,000 people or sensitive personal information of a cumulative total of 10,000 people since January 1 last year is to provide personal information abroad; (4) Other circumstances where a security assessment of cross-border data transfer is required as prescribed by the State cyberspace department. Article 5 Before a data handler applies for a security assessment of cross-border data transfer, it shall carry out a risk self-assessment over the cross-border transfer of data, with a focus on: (1) The legitimacy, justifiability and necessity in the purpose, scope, method, etc. of the crossborder transfer of data and of the data processing by the overseas recipient; (2) The scale, scope, type, and sensitivity of the data to be transferred abroad, and the risks the cross-border transfer of data could pose to national security, public interests, or the legitimate rights and interests of individuals or organizations; (3) The responsibilities and obligations the overseas recipient commits itself to undertake, and whether its management and technical measures and capabilities for performing such responsibilities and obligations can ensure the security of the data to be transferred abroad; (4) The risk of data being tampered with, corrupted, leaked, lost, transferred, or illegally accessed or illegally used during and after the cross-border transfer, and whether there are obstacles in protecting personal information rights and interests; (5) Whether the contract for cross-border data transfer to be concluded with the overseas recipient or other documents with legal effect (hereinafter referred to collectively as “legal documents”) have fully specified the responsibilities and obligations for data security protection. (6) Other matters that could impact the security of cross-border data transfer.	Outbound Data Transfer Security Assessment Measures (DigiChina Translation here) Original Texts: http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm ; http://www.cac.gov.cn/2022-07/07/c_1658811536800962.htm

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
		Article 6 When applying for a security assessment over cross-border transfer of data, the applicant shall submit the following materials: (1) Written application; (2) Risk self-assessment report on cross-border data transfer; (3) Legal documents to be concluded between the data handler and the overseas recipient; (4) Other materials required for security assessment. Article 7 Cyberspace departments at the provincial level shall, within five working days of the date of receiving the application materials, complete the examination of their completeness. Where the application materials are found complete, they shall be submitted to the State cyberspace department; if not, they shall be returned to the data handler, and a oneoff notice shall be given regarding materials to be supplemented. The State cyberspace department shall, within seven working days of the date of receiving the application materials, decide whether to accept the application for assessment and notify the data handler of its decision in writing. Article 8 The security assessment of crossborder data transfer shall focus on the risks that the cross-border transfer of data could pose to national security, public interests, or the legitimate rights and interests of individuals or organizations, mainly including: (1) The legitimacy, justifiability and necessity of the purpose, scope, method, etc. of the crossborder transfer of data; (2) The impact of the policies and regulations on data security protection and the cybersecurity environment in the country/region where the overseas recipient is located on the security of the data to be transferred abroad; whether the data protection provided by the overseas recipient meets the requirements as specified in the laws, administrative regulations and mandatory national standards of the People's Republic of China; (3) The scale, scope, type, and sensitivity of the data to be transferred abroad, and the risk of data being tampered with, corrupted, leaked, lost, transferred, or illegally accessed or illegally used during and after the cross-border transfer; (4) Whether data security and personal information rights and interests can be fully and effectively protected; (5) Whether the legal documents to be concluded between the data handler and the overseas recipient has adequately specified the responsibilities and obligations for data security protection; (6) The compliance with the laws, administrative regulations, and departmental rules of China; (7) Other matters that the State cyberspace department deems to require an assessment. Article 9 The responsibilities and obligations for data security protection shall be specified by the data handler in the legal document concluded with the overseas recipient, at least including: (1) The purpose and method of the crossborder transfer of data and the scope of the data to be transferred, the purpose and method of the data processing by the overseas recipient, etc.; (2) The location and period of overseas storage of data, and the measures for dealing with the transferred data after the storage period expires, the agreed purpose is fulfilled, or the legal document is terminated; (3) The restrictive requirements for the retransfer of the transferred data by the overseas recipient to other organizations or individuals; (4) The security measures that should be taken when it is difficult to ensure data security due to a substantial change to the de facto control or business scope of the overseas recipient, or a change to the data security protection policy and regulations and cybersecurity environment, or due to other force majeure events in the country/region where the overseas recipient is located; (5) The remedial measures, liability for breach of contract, and the dispute settlement method in case of a violation of the data security protection obligations specified in the legal documents; (6) The requirements for carrying out emergency response actions properly in case of risks of cross-border data being tampered with, corrupted, leaked, lost, transferred, or illegally accessed or illegally used, and the routes and methods for individuals to protect their personal information rights and interests. Article 10 After accepting an application, the State cyberspace department shall, based on the application details, organize relevant departments under the State Council, the provincial-level cyberspace department, and specialized organizations to conduct a security assessment. Article 11 Where, during a security assessment, the State cyberspace department finds the application materials submitted by a data handler fail to comply with relevant requirements, it may require it to submit more or make corrections. Where the data handler, without justifications, does not submit more or make corrections, the State	

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
		cyberspace department may terminate the security assessment. The data handler shall be responsible for the authenticity of submitted materials. Should it submit false materials, it shall be deemed to fail the assessment, and be held legally accountable according to law. Article 12 The State cyberspace department shall, within 45 working days of the date of issuing a written notice on accepting the application to relevant data handler, complete the security assessment of cross-border data transfer; the assessment may be properly extended in complicated cases or if supplementary materials or corrections are required, and the expected duration of the extension shall be notified to the data handler. The assessment result shall be notified to the data handler in writing. Article 13 Should a data handler have an objection to the assessment result, it may, within 15 working days of the date of receiving the assessment result, apply to the State cyberspace department for a re-assessment, and the re-assessment conclusion is final. Article 14 A Yes conclusion on cross-border data transfer is valid for two years. Under any of the following circumstances within the period of validity, the data handler shall reapply for an assessment: (1) A change occurs to the purpose, method, scope, or category of the cross-border transfer of data or the purpose or method of the data processing by the overseas recipient, impacting the security of the data to be transferred abroad, or the period for overseas storage of personal information and critical data is extended; (2) A change occurs to the data security protection policy and regulations and cybersecurity environment, or other force majeure events occur in the country/region where the overseas recipient is located, or a change occurs to the de facto control of the data handler or overseas recipient, or to the legal document concluded between the data handler and the overseas recipient, which has an impact on the security of the data to be transferred abroad; (3) Other circumstances having an impact on the security of the data to be transferred abroad. Where the data handler needs to continue the original cross-border transfer of data after the expiry of the validity period, it shall re-apply for an assessment 60 working days prior to the expiry of the validity period. Article 15 The relevant organizations and personnel participating in security assessment shall, according to law, keep confidential the data such as State secrets, personal privacy, personal information, trade secrets, and confidential business information they have accessed in the course of performing their duties, and shall not disclose or illegally provide the data to others, or illegally use the data. Article 16 Where any organization or individual finds that a data handler provides data abroad in violation of these Measures, it/he may complain to or tip off the cyberspace department at or above the provincial level. Article 17 Where the State cyberspace department finds that, during the actual processing, a cross-border transfer of data already passing the assessment no longer meets the security management requirements for cross-border data transfer, it shall notify the data handler in writing to terminate the crossborder transfer of data. Where the data handler needs to continue the cross-border transfer of data, it shall make rectifications as required, and re-apply for an assessment after the rectification. Article 18 In case of a violation of the provisions of these Measures, the case shall be dealt with in accordance with laws and regulations such as the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic ofChina, and the Law of the People's Republic of China on Personal Information Protection; to the extent that the violation constitutes a crime, the violator shall be subject to criminal liability according to law. Article 19 For the purpose of these Measures, critical data refers to the data whose tampering, corruption, leaks or illegal access or illegal use could endanger national security, economic operation, social stability, public health and security, etc.	
Online Data Security Management Regulations (Draft for Comment) (Nov. 2021)	Various	Summary: The **Online Data Security Management Regulations** were released in draft for Comment in November 2021. Key provisions are summarized below. Article 35: Data transfers are subject to fulfillment of one of the following conditions: (1) the transferor must pass a CAC security assessment; (2) transferor and transferee must be certified by a professional organization recognized by CAC; (3) transferor and transferee have concluded a CAC-formulated standard contract; or (d) other legal conditions. Article 39 proscribes: (1) the transfer of personal information beyond the purpose, scope, method, data type and scale specified in the impact assessment report submitted to CAC; and (2) the transfer of personal information and important data abroad beyond the purpose, scope, method, data type and scale specified in the	Draft Network Data Security Administrative Regulation (translation here).

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
		CAC-conducted security assessment; and (3) the provision of any data stored within China to foreign judicial or law enforcement agencies, absent advance approval by relevant Chinese authorities. Article 39 also requires: (1) adoption of effective measures (e.g., contracts) to supervise the use of the data and the performance of data security protection obligations by the data recipient; (2) processes to address user complaints related to data cross-border transfer; (3) assumption of legal liability for any damage that the cross-border transfer causes to the public interest or individual rights/interests; (4) maintenance of transfer logs and approvals for at least three years; and (5) a clear display – per CAC instructions – of the type and scope of personal information/important data being transferred. Article 40 imposes obligations to provide CAC with a data cross-border transfer security report on an annual basis. <u>Excerpt</u>: Chapter V: Cross-Border Data Security Management Article 35: Where data handlers need to provide data outside of the territory of the People's Republic of China due to operational and other such requirements, they shall meet one of the following conditions: 1. Undergoing a data cross-border security assessment organized by the national cybersecurity and informatization department; 2. The data handler and data recipient both passing personal information protection certification conducted by a specialized body recognized by the national cybersecurity and informatization department; 3. Concluding contracts with the foreign data recipient according to provisions formulated by the national cybersecurity and informatization department concerning standard contracts, defining both sides' rights and obligations; 4. Other conditions provided by law, administrative regulations, or the national cybersecurity and informatization department. Where a data handler provides personal information of a concerned party abroad as required for concluding or fulfilling a contract where an individual is a concerned party, or personal information is provided abroad as necessary for protecting individuals' lives or health, or the security of their property, an exception is made. Article 36: Where data handlers provide personal information outside of the territory of the People's Republic of China, they shall notify the individual about the name of the foreign data recipient, their contact method, the handling purpose, handling method, personal information categories, as well as methods for individuals to exercise their personal information rights with the foreign data recipient and other such matters, and obtain separate consent from the individual. Where individuals' consent has been obtained separately for personal information export at the time of personal information collection, and export takes place according to the matters for which consent has been obtained, it is not necessary to obtain the individual's separate consent again. Article 37: Where data handlers provide data collected or produced within the territory of the People's Republic of China abroad, and the matter falls under the following circumstances, they shall undergo a data cross-border security assessment organized by the national cybersecurity and informatization department: 1. The data transferred abroad contains important data; 2. Critical information infrastructure operators, or data handlers handling the personal information of 1 million or more persons, providing personal information abroad; 3. Other circumstances as provided by the national cybersecurity and informatization department. Where laws, administrative regulations or the national cybersecurity and informatization department provide it is permitted to not conduct a security assessment, those provisions are followed. Article 38: Where the People's Republic of China has concluded or acceded to international treaties or agreements that contain provisions concerning the conditions for providing personal information outside of the territory of the People's Republic of China, it is permitted to act according to those provisions. Article 39: Data handlers shall fulfill the following duties when providing data abroad:	

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
		1. They may not provide personal information abroad outside of the purpose, scope, method, data categories, scale, etc., indicated in the report submitted to the cybersecurity and informatization department concerning personal information protection impact assessment; 2. They may not provide personal information or important data abroad in excess of the export purpose, scope, method and data categories, scope, etc., determined at the time of security assessment by the cybersecurity and informatization department; 3. Adopt contracts and other such effective measures to supervise data recipients to use data according to the purpose, scope, and method agreed upon by both parties, fulfill data security protection duties, and ensure data security; 4. Accepting and handling outbound data transfer-related user complaints; 5. Where outbound data transfer generates harm to the lawful rights and interests of individuals or organizations, or the public interest, data handlers shall bear liability according to the law; 6. Retaining related daily records and outbound data transfer examination and approval records for a period of three years or more; 7. When the national cybersecurity and informatization department, together with relevant State Council departments, examine and verify the categories and scope of personal information and data provided abroad, data handlers shall provide explanations in clear writing and in readable ways; 8. Where cybersecurity and informatization departments determine outbound transfer is not permitted, data handlers shall cease outbound data transfer, and adopt effective measures to supplement the security of data already transferred abroad; 9. Where personal information needs to be transferred after outbound transfer, the conditions for re-transfer shall be agreed upon with the individual in advance, and the security protection duties the recipient is to fulfill clarified. Without the approval of the competent department of the People's Republic of China, domestic individuals and organizations may not provide data stored within the territory of the People's Republic of China to foreign judicial and law enforcement bodies. Article 40: Data handlers providing personal information and important data abroad shall compile an outbound data transfer security report before January 31 of each year, and report the data export situation of the previous year to the districted city-level cybersecurity and informatization department: 1. The complete name and contact method of the data recipient; 2. The categories, quantities, and purpose of the exported data; 3. The storage location, storage period, and scope and methods of use of the data abroad; 4. The situation of user complaints involving foreign provision of data and their handling situation; 5. Occurred data security incidents and their response situation; 6. The situation of retransfer after data export; 7. Other matters required to be reported by the national cybersecurity and informatization department concerning provision of data abroad. Article 41: The State establishes a cross-border data security gateway, to interrupt the transmission of information originating from outside the People's Republic of China, of which laws and administrative regulations prohibit the dissemination or transmission. No individual or organization may provide software, tools, lines (线路), etc., used to penetrate or circumvent the cross-border data security gateway; they may not provide Internet access, server contracting, technical support, dissemination and marketing, payment settlement, application download, and other such services for the penetration or circumvention of the cross-border data security gateway. Where domestic users access the domestic network, their flow may not be routed abroad. Article 42: Data handlers engaging in cross-border data activities shall, according to the supervision and management requirements for national cross-border data security supervision and management, establish and complete related technical and management measures. -- Article 13: Data handlers conducting the following activities shall report for cybersecurity review according to relevant State provisions: 1. Where Internet platform operators collecting or holding large amounts of data resources related to national security, economic development, or the public interest, carry out mergers, reorganizations, or separations, affecting or possibly affecting national security;	

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
		2. Where data handlers handling personal information of more than 1 million individuals list on a market abroad; 3. Where data handlers list in Hong Kong, affecting or possibly affecting national security; 4. Other data handling activities affecting or possibly affecting national security. Large-scale Internet platform operators establishing headquarters or operations centers, or research and development centers, abroad, shall report the matter to the national cybersecurity and informatization department and competent department. ... Article 32: Data handlers handling important data or listing on stock exchanges abroad shall conduct a data security assessment once every year themselves, or entrust a data security service body to do so, and submit the data security assessment report of the previous year to the districted city-level cybersecurity and informatization department by January 31 every year; the annual data security assessment report's content includes: 1. The situation of handling important data; 2. Discovered data security risks and response measures; 3. Data security management systems, data back-up, encryption, access control, and other such security protection measures, as well as the management system implementation situation and the efficacy of protective measures; 4. The situation of implementing national data security laws, administrative regulations and standards; 5. The situation of occurred data security incidents and their handling; 6. The security assessment situation of important data sharing, trading, entrusted handling, and provision abroad; 7. Data security-related complaints and the handling situation; 8. Other data security matters determined by the national cybersecurity and informatization department and competent and supervision departments. Data handlers shall preserve risk assessment reports for at least three years. On the basis of departmental divisions of duties and responsibilities, cybersecurity and informatization departments are to share reported information with relevant departments. Data handlers conducting security assessment for important data sharing, trading, entrusted handling, or provision abroad, shall focus on assessing the following content: 1. The data shared, traded, entrusted for handling, or provided abroad, as well as whether the purpose, method, scope, etc., of the data recipient's data handling are lawful, proper, and necessary; 2. The risk that the data shared, traded, entrusted for handling, or provided abroad leaks, or is destroyed, distorted, or abused; as well as the risks brought to national security, economic development, and the public interest; 3. The trustworthiness status and legal compliance system of the data recipient, their cooperative relationship with foreign government bodies, whether or not they are sanctioned by the Chinese government, and other such background information, whether or not they are able to effectively protect data security through the responsibility they commit to bear as well as their capability to fulfill their responsibilities, etc.; 4. Whether the requirements concerning data security in the related contracts concluded with the data recipient can effectively restrain the data recipient to fulfilling their data security protection duties and responsibilities; 5. Whether or not management and technical measures during the data handling process can prevent data leaks, destruction, and other such risks. Where the assessment establishes that harm to national security, economic development, or the public interest is possible, data handlers may not share data, trade it, entrust its handling, or provide it abroad.	
Cyberspace Administration of China, Draft Standard Contract	Personal information	**Provisions on Standard Contract for Personal Information Cross-border Transfer** (Draft for comments)	Cyberspace Administration of China, Draft Standard Contract

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
Provisions (July 2022), at: http://www.cac.gov.cn/2022-06/30/c_1658205969531631.htm		Article 1 For the purpose of regulating the personal information cross-border transfer activities, safeguarding personal information rights and interests, and promoting the safe and free flow in personal information cross-border transfer, these Provisions are formulated in accordance with the Personal Information Protection Law of the People's Republic of China. Article 2 Where a personal information handler, pursuant to Subparagraph (3) of the first paragraph of Article 38 of the Personal Information Protection Law of the People's Republic of China, concludes a contract with an overseas recipient to provide personal information abroad, a standard contract for personal information cross-border transfer shall be signed in accordance with these Provisions (hereinafter referred to as the "standard contract"). Other contracts related to activities of personal information cross-border transfer signed between the personal information handler and the overseas recipient shall not conflict with the standard contract. Article 3 In carrying out personal information cross-border transfer activities according to the standard contract, it is necessary to ensure that the concluding of this Contract is voluntary and subject to the filing management system, guard against the security risks of personal informationcross-border transfer, and ensure the lawful, orderly and free flow of personal information. Article 4 Should a personal information handler conform to all of the following circumstances, it may provide personal information abroad by signing a standard contract: (1) It is a non-critical information infrastructure operator; (2) The personal information it processes is of less than 1 million people; (3) The cumulative personal information it provides abroad is of less than 100,000 people since January 1 of the previous year; (4) The cumulative sensitive personal information it provides abroad is of less than 10,000 people since January 1 of the previous year. Article 5 Before providing personal information abroad, a personal information handler shall conduct an impact assessment on personal information protection in advance, with a focus on the following: (1) The legitimacy, justifiability and necessity of the purpose, scope, method, etc. of processing personal information by the personal information handler and the overseas recipient; (2) The volume, scope, type and sensitivity of personal information to be transferred abroad, and the risks that may be brought about by the cross-border transfer of personal information to the personal information rights and interests; (3) The responsibilities and obligations the overseas recipient has committed to undertake, as well as whether the management and technical measures, capabilities, etc. to fulfill the obligations can ensure the security of personal information to be transferred abroad; (4) The risks of personal information being divulged, damaged, tampered with and abused after cross-border transfer, whether the channels for individuals to safeguard their personal information rights and interests are unobstructed, etc.; (5) Impact of personal information protection policy & regulations in the overseas recipient’s home country/region on the performance of the standard contract; (6) Other matters that may impact the security of personal information cross-border transfer. Article 6 A standard contract includes the following main contents: (1) Basic information of the personal information handler and overseas recipient, including but not limited to their names and addresses, and the name and contract information of their contact persons; (2) The purpose, scope, types, sensitivity, volume, method, storage period and storage location regarding cross-border transfer of personal information; (3) The responsibility and obligations of the personal information handler and overseas recipient for personal information protection, and technical and management measures taken to prevent security risks possibly brought by the cross-border transfer of personal information; (4) Impact of personal information protection policy & regulations in the overseas recipient’s home country/region on compliance with this Contract; (5) Rights of the personal information subject, and the ways/methods of protecting the rights of personal information subjects; (6) Means of relief, contract cancellation, liability for breach of contract, dispute settlement, etc. Article 7 A personal information handler shall, within 10 working days of the date of entry into force of the standard contract, file with the local cyberspace department at the provincial level. The following materials shall be submitted for the record-filing: (1) A standard contract; (2) The impact assessment report on the personal information protection. The personal information handler shall be responsible for the authenticity of the materials filed. The personal information handler can carry out personal information cross-border transfer activities after the standard contract comes into effect.	Provisions (July 2022), at: http://www.cac.gov.cn/2022-06/30/c_1658205969531631.htm

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
		Article 8 Under any of the following circumstances within the validity period of the standard contract, the personal information handler shall re-sign a standard contract and go through the filingprocedure: (1) There is a change in the purpose, scope, types, sensitivity, volume, method, storage period and storage location regarding the provision abroad of personal information, as well as the use of personal information and the method of the overseas recipient's processing personal information; or the overseas storage period of personal information is extended; (2) The personal information protection policy & regulations in the overseas recipient's home country/region change, which may affect the personal information rights and interests; (3) Other circumstances that may affect the personal information rights and interests. Article 9 Institutions and personnel involved in the record-filing of the standard contract shall keep confidential the personal privacy, personal information, trade secrets and confidential business information that they have accessed in the course of performing their duties, and shall not divulge them or illegally provide them to others or illegally use them. Article 10 Any organization or individual who finds that a personal information handler violates these Provisions shall have the right to complain to or tip off the cyberspace departments at or above the provincial level. Article 11 Where a cyberspace department at or above the provincial level finds that a personal information cross-border transfer activity conducted according to a concluded standard contract, in the actual processing process, no longer meets the security management requirements for personal information cross-border transfer, it shall notify the personal information handler in writing to terminate the personal information cross-border transfer activity. The personal information handler shall terminate the personal information cross-border transfer activity immediately after receiving the notification. Article 12 Where a personal information handler, in accordance with these Provisions, concludes a standard contract with the overseas recipient to provide personal information abroad, under any of the following circumstances, the cyberspace departments at or above the provincial level shall, pursuant to the provisions of the Personal Information Protection Law of the People's Republic of China, order it to make corrections within a specified time limit; where it refuses to make corrections or impairs the personal information rights and interests, ordered it to stop the personal information cross-border transfer activity and impose punishment according to law; to the extent that the violation constitutes a crime, it shall be subject to criminal liability according to law. (1) Failing to perform the record-filing procedures, or submitting false materials for the recordfiling; (2) Failing to perform the responsibilities and obligations stipulated in the standard contract, infringing upon the personal information rights and interests and causing damage; (3) Other circumstances affecting the personal information rights and interests arise.	

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
Measures for Data Security Management in the Fields of Industry and Information Technology	"Key data", "Core data"	**China – Measures for Data Security Management in the Fields of Industry and Information Technology (Trial):** On January 1, 2023, China's Measures for Data Security Management in the Fields of Industry and Information Technology went into effect. This final version of the Measures was released on December 13, 2022, and includes data localization mandates and cross-border data transfer restrictions of varying degrees of severity for "general data," "key data," and "core data," which are defined in Articles 9-11, respectively. Potentially with scope are: (1) Industrial data generated and collected in the process of R&D and design, production and manufacturing, operation management, maintenance, etc.; (2) Telecommunications data; (3) Radio data, including radio frequency, station, other radio wave parameter data generated and collected during radio business activities. Affected entities include: (1) industrial enterprises; (2) Software and IT service enterprises; (3) Telecommunication business operations; (4) Station operators holding a telecommunication business license. Relevant cross-border data provisions are specified below (emphasis added). • Article 12: Data handlers in the fields of industry and information technology shall file their own catalogs of key data and core data with the sector-specific regulatory department in their own regions. The contents of filing shall include but not limited to the basic information of data such as sources, categories, levels, size, carriers, handling purposes and methods, use scope, responsible subjects, outbound sharing, cross-border transfer, and security protection measures, exclusive of the data content itself. • Article 21: The key data and core data generated and collected by the data handlers in the fields of industry and information technology within the territory of the People's Republic of China shall be stored within the territory of the People's Republic of China if laws or administrative regulations have such requirements. *Should the data need to be provided abroad, a data cross-border transfer security assessment shall be carried out* according to laws and regulations. ... Without the approval of the Ministry of Industry and Information Technology, the data handlers in the fields of industry and information technology shall not provide foreign industrial, telecommunication and radio law enforcement agencies with data in the fields of industry and information technology that is stored within the territory of the People's Republic of China. • Article 24: In case of cross-entity provision, transfer or entrusted handling of core data, the data handler in the fields of industry and information technology shall assess security risks, and take necessary security protection measures; the case shall be reviewed by the sector-specific regulatory department in the region and reported to the Ministry of Industry and Information Technology. The Ministry of Industry and Information Technology shall conduct review according to the relevant regulations. • Article 31: The Ministry of Industry and Information Technology shall develop a sector-specific data security assessment management system to manage the assessment institutions; develop a specification for assessment of sector-specific data security, to guide the assessment institutions to carry out data security risk assessment, cross-border transfer security assessment and other work. The local sector-specific regulatory departments shall be responsible for carrying out the data security assessment work in their own regions respectively. The key data and core data handlers in the fields of industry and information technology shall conduct risk assessment on the data handling activities at least once a year on their own or by entrusting a third-party assessment institution, make timely rectifications over risk issues, and send a risk assessment report to the sector-specific regulatory department in their own regions.	Measures for Data Security Management in the Fields of Industry and Information Technology, http://www.gov.cn/zhengce/zhengceku/2022-12/14/content_5731918.htm

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
Specification for Security Certification of Personal Information Cross-Border Processing, (V2.0-202212),	"Personal information"	**China – Technical Specification for Cross-Border Processing of Personal Information:** On December 16, 2022 China released the Specification for Security Certification of Personal Information Cross-Border Processing (V2.0-202212). The Specification is a "standards-related technical document developed and issued by the Secretariat of the National Information Security Standardization Technical Committee (TC260)." The Specification applies to personal information handlers carrying out cross-border handling activities of personal information, and it serves as the certification basis for certification bodies to conduct personal information protection certification for cross-border handling activities of personal information (Art. 1). It defines "personal information handler" as an organization or individual who independently decides the purpose and method of handling in the handling of personal information, and it defines "overseas recipient" as an organization or individual located outside China and receiving personal information from personal information handlers. It states in relevant part as follows (emphasis added): In carrying out cross-border processing activities, personal information handlers applying for personal information protection certification shall comply with the requirements of *GB/T 35273 Information security technology – Personal information security specification* and this document. This document … provides a basis for certification bodies to conduct an assessment over personal information cross-border processing activities of personal information handlers, and providing reference for personal information handlers to lawfully carry out personal information cross-border processing activities as well. … Personal information handlers who apply for certification shall obtain a lawfully issued legal person certificate, operate normally and have a good reputation and goodwill. Where a personal information cross-border processing activity takes place between subsidiaries or affiliates of a multinational or an economic or noneconomic entity, the party located in China may apply for certification, and assumes legal liability. For an overseas personal information processor specified in the second paragraph of Article 3 of the Personal Information Protection Law of the People's Republic of China, its China-based office or its designated representative may apply for certification, and assumes legal liability. A legally binding and enforceable document shall be entered into between the personal information handler and the overseas recipient in a personal information cross-border processing activity, to ensure the rights and interests of personal information subjects are fully protected. The document shall at least specify the following contents: a) Basic information of the personal information handler and the overseas recipient, including but not limited to name, address, contact person's name, contact information, etc.; b) Purpose of the cross-border processing of personal information, and the scope, types, sensitivity, volume, processing method, retention period, storage location and the like of personal information; c) Responsibilities and obligations of the personal information handler and the overseas recipient for personal information protection, technical and management measures taken to prevent possible security risks caused by the cross-border processing of personal information, etc.; d) Rights of personal information subjects, and the ways and methods to protect the rights of the personal information subjects; e) Remedy, cancellation of contract, liability for breach of contract, dispute settlement, etc.; f) The overseas recipient undertakes to honor the same personal information cross-border processing rules, and ensures that the protection of personal information is not lower than the standard specified in the laws and administrative regulations of the People's Republic of China on personal information protection; g) The overseas recipient undertakes to subject itself/himself to the continuous supervision of the personal information cross-border processing activities by the certification body; h) The overseas recipient undertakes to accept the jurisdiction of the laws and administrative regulations of the People's Republic of China on personal information protection; i) Clarifying the organization assuming legal liability within the territory of the People's Republic of China, and undertaking to fulfill the obligation of personal information protection; j) Both the personal information handler and the overseas recipient undertake to assume civil legal liability for the infringement of the personal information rights and interests, and explicitly agree on the civil legal liability to be borne by both parties; k) Other obligations that are specified by laws and administrative regulations and shall be fulfilled.	Specification for Security Certification of Personal Information Cross-Border Processing, (V2.0-202212), https://www.tc260.org.cn/front/postDetail.html?id=20221216161852
Cybersecurity Requirements for Critical Information Infrastructure	Personal information, important data, critical information	**China – National Technical Standard re Cybersecurity Requirements for Critical Information Infrastructure Protection:** On November 7, 2022 the TC260 National Information Security Standardization Technical Committee announced that the State Administration for Market Regulation and National Standardization Administration had issued (on October 28), a technical standard entitled Information security technology - Cybersecurity Requirements for Critical Information Infrastructure Protection (GB/T 39204-2022). This is reportedly China's first national standard for critical information infrastructure ("CII") security protection. It establishes cybersecurity requirements for CII protection in areas such as analysis and identification, security protection, testing and evaluation, monitoring and early warning, active defense, incident disposal, etc., aiming	Cybersecurity Requirements for Critical Information Infrastructure

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
Protection (GB/T 39204-2022)		to take necessary measures to protect the continuous operation of CII business and its important data from damage. The technical standard includes the following "data security" requirements (emphasis added): Requirements for data security protection include: a) Shall establish data security management responsibilities and appraisal and assessment system, prepare data cybersecurity plan, implement data security technology protection, carry out data security risk assessment, develop data security incident emergency plans, dispose of security incidents in a timely manner, and organize data security education and training. b) Shall establish data cybersecurity policies based on data categorization and classification, and specify the corresponding measures for the protection of important data and personal information. c) Personal information and important data collected and generated during operations in China will be stored within the territory of China. If, due to business needs, it is necessary to provide data abroad, security assessment shall be conducted in accordance with the relevant national regulations and standards. Where there are other provisions in laws or administrative regulations, such provisions shall prevail. d) Shall strictly control the use, processing, transmission, provision and disclosure and other key aspects of important data, and adopt encryption, desensitization, de-identification and other technical means to protect the security of sensitive data. e) Business continuity management and disaster recovery backup mechanisms shall be established, and important systems and databases shall be backed up off-site. f) If the data availability requirement is high, the database remote real-time backup measures shall be taken, and if the business continuity requirement is high, the system remote real-time backup measures shall be taken to ensure that once the critical information infrastructure is damaged, it can be restored and remedied in a timely manner. g) When the critical information infrastructure is decommissioned, the stored data shall be processed in accordance with the data security protection policies. h) The security capability of the whole process of data processing activities shall be established, which shall comply with the requirements of relevant national standards on data cybersecurity protection	Protection (GB/T 39204-2022), https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=1D986D9DCCC518D19DAD9431DD76053E
Implementation Rules for Personal Information Protection Certification	Personal information	**China – Implementation Rules for Personal Information Protection Certification (PI Certification Rules):** On November 18, 2022, the Cyberspace Administration of China (CAC) and the State Administration of Market Regulation (SAMR) announced the publication (with immediate effect) of the Personal Information Certification Rules. These rules are intended to support the Personal Information Protection Law (PIPL), outlining requirements for the certification of personal information processors to carry out personal information collection, storage, use, processing, transmission, provision, disclosure, deletion, cross-border, and other processing activities. As a procedural matter, the rules provide for a Certification Implementation Process, which includes: (1) a certification application process, (2) a technical verification of the application by the technical verification body, (3) an on-site audit, (4) the certification body's certification decision (based on an assessment and approval of certification results), and (5) post-certification supervision. As a substantive matter, the Rules mandate compliance with the GB/T 35273 Information Security Technology Personal Information Security Specification, for personal information processors conducting cross-border processing activities, they should also comply with the requirements of TC260-PG-20222A Specification for Security Certification of Personal Information Cross-Border Processing Activities.	http://www.cac.gov.cn/2022-11/18/c_1670399936983876.htm Additional coverage here: Reed Smith, ODP, Han Kun, Bird & Bird.
City of Beijing Municipal Regulations on the Promotion of Digital Economy		**China – Beijing Municipal Regulations on the Promotion of Digital Economy:** On November 25, 2022 the City of Beijing published Municipal Regulations on the Promotion of Digital Economy in order to "turn Beijing into a global benchmark city in practicing digital economy." Relevant provisions include: • Article 29: The commerce department shall, in conjunction with relevant departments, promote the high-quality development of digital trade, ...support the development of cross-border trade, cross-border logistics and cross-border payments, boost the international mutual recognition of digital certificates and electronic signatures, construct international Internet data dedicated channels, international data and information dedicated channels and application support platforms based on advanced technologies such as blockchain so as to provide facilitation for the product delivery and settlement in digital trade. • Article 48: In carrying out data processing activities, an entity shall establish a data governance and compliance operation system, fulfill data security protection obligations, strictly implement relevant systems such as those regarding legal use of personal information, the commitment to the safe use of data and the security management over cross-border transfer of key data, and based on application scenarios, conduct a security assessment over anonymization and de-identification technologies, and take necessary technical measures to strengthen the protection of personal information security, to prevent illegal abuse.	City of Beijing, Municipal Regulations on the Promotion of Digital Economy http://www.bjrd.gov.cn/xwzx/cwhgg/202211/t20221128_2867338.html

Title	Types of Data Covered	Selected Rules in China on Cross-Border Data Transfers or Data Localization	Sources
		• Article 56: Work to encourage the expansion of international cooperation in the field of digital economy, support participation in the development of international rules, standards and agreements, set up cooperation platforms such as international exhibitions, forums, commerce & trade fairs, competitions and training, and achieve mutual benefit and win-win cooperation in the fields of cross-border flow of data, opening up of the digital service market, and digital product security certification	
Internet Medical and Health Information Security Management Specifications	Health	The National Health Commission of the People's Republic of China has published measures on **Internet Medical and Health Information Security Management Specifications** (国家卫生健康委统计信息中心关于征求《互联网医疗健康信息安全管理规范（征求意见稿）》标准意见). These draft measures contain data localization provisions modelled on the Data Security Law and draft Personal Information Protection Law. Similar to the approach taken in the Automotive Data Management Regulations, the measure requires storage of personal and important data in China, as follows: Personal information and important data collected and generated during the process and operation of Internet health care services should be stored in China. If, due to business needs, it is necessary to provide it abroad, a safety assessment shall be conducted in accordance with the methods formulated by the State Internet And Communications Department in conjunction with the relevant departments of the State Council, but if otherwise provided by laws and administrative regulations, it shall be administered in accordance with the relevant provisions.	National Health Commission, *Internet Medical and Health Information Security Management* Specifications
Data Management Rules for Automotive Applications	Auto-motive	Summary: Under the ***Data Management Rules for Automotive Applications*****,** which became effective on October 1, 2021, require operators (e.g., automotive OEMs, etc.) to store personal data and important data in China. If strictly necessary, the operator may seek an exception from this rule based on an official approval for such transfer following a cross-border transfer security assessment conducted by government authorities. (ADMR, Art. 12). Operators are subject to strict legal obligations in connection with any transfer (supervising foreign data recipients; legal liability; data type, scope, use, and process limitations; governmental reporting requirements, etc.) (ADMR, Arts. 13-19).	Data Management Rules for Automotive Applications
Connected Vehicle Data Security Requirements	Auto-motive	Summary: Under the ***Connected Vehicle Data Security Requirements*****,** there is a strict prohibition of any cross-border transfer of Data relating to roads, buildings, topography, traffic participants, among others, and the vehicle location and track data, collected by a connected vehicle from the environment outside the vehicles through cameras, radar and other sensors (CVSDR, Art. 7.1).	
Notice on Strengthening Internet of Vehicle Cybersecurity and Data Security	Auto-motive	Summary: Under the ***Notice on Strengthening Internet of Vehicle (IoV) Cybersecurity and Data Security,*** *which are intended* to support the implementation of the *New Energy Vehicle Industry Development Plan (2021-2035)*, ICV manufacturing enterprises and IoV service platform operation enterprises are required to conduct a cross border data transfer security assessment if they wish to provide important data abroad.	
14th Five-Year Big Data Industry Development Plan	Various	Summary: On November 30, the Ministry of Industry and Information Technology ('MIIT') issued a notice on the 14th Five-Year Big Data Industry Development Plan. The Plan purports to improve data security with a focus on data classification, the monitoring of sensitive data leakage, and illegal cross-border data flow, as well as privacy enhanced technologies, data de-sensitization, and other data security techniques. The Plan also provides for a Data Security Casting Shield Operation that comprises cross-border data transmission security mechanisms, which include security risk assessments and pilot programs in particular regions for international cooperation of cross-border data security rules.	Notice on the 14th Five-Year Big Data Industry Development Plan
Information Security Technology — Identification Guide of Important Data.	Various	Summary: On September 23, China's National Information Security Standardization Technical Committee, the drafters of China TC260 standards, issued the Information Security Technology — Identification Guide of Important Data. The Guide seeks to implement the Data Security Law, which imposes cross-border data restrictions and security assessment requirements on "important" data. The Guide outlines the principles, framework and rules for data categorization and classification from the perspective of national data security management. The Guide introduces different data categories such as: important (or "key") data, core national data, personal information, public data, corporate data and derivative data. Different categories of data should also be classified into five levels based on the risk of harm and type of harm it caused (national security, public interests, legitimate rights and interests of individuals, and legitimate rights and interests of organizations)	Information Security Technology — Identification Guide of Important Data.
14th Five-Year Plan (MOFCOM)	Various	On October 21, MOFCOM issued its 14th Five-Year Plan, which prioritizes digital trade expansion. In the Plan, MOFCOM pledges "to support the trade of digital products, to foster a good environment for digital products to go overseas, and to explore the trading of data." The SCMP further reports that, "China's digital trade volume increased 47.4 per cent to US$294.76 billion in 2020, up from US$200 billion in 2015, according to data from Mofcom. The share of digital trade in the country's overall trade in services grew to 44.5 per cent in the same five-year period, compared with 30.6 per cent previously. The nation's digital economy was worth 39.2 trillion yuan (US$6.1 trillion) last year, a 3.3 trillion yuan increase from 2019."	

Comparison of PIPL, DSL, and Automotive Data Mgmt Rules

	Personal Information Protection Law	Data Security Law	Automotive Data Management Regs (ADMR) / Connected Vehicle Data Security Requirements (CVDSR)
Extraterritorial Application?	Yes	Yes	Yes
Scope of Covered Data?	"Personal info" is any information that can identify natural persons	"Important data" is any record of information deemed to be "important" from perspective of economic, social, national security, public interest, or private interests.	"Personal data" is any data about the owner, driver, driver, passenger, pedestrian, etc.; "Important data" includes data from official facilities, mapping data, data on vehicle flows/types on roads, and voice over video data, and other public interest data.
Do Safety/ Security/ Risk Assessments Require Official Notification/ Approval?	Sometimes. • Official approval of safety assessment required prior to any cross-border data transfers. (Art. 38). • Official approval of security assessment required for CII operators and large-scale personal data processors (Art. 40) • Personal information risk assessment records to be retained by processors for at least 3 years (Art. 54).	Yes. • Official notification/transmittal required for important data risk assessment reports	Yes. • State cyberspace department shall, in conjunction with other departments, conduct a data security assessment
Are Data Localization Mandates and/or Data Transfer Restrictions Imposed?	Yes. • Critical Information Infrastructure (CII) operators and large-scale personal data processors must store data in China, and may only transfer data with official approval (Art. 40) • Personal information processors may only transfer data overseas if they conduct an officially-organized safety assessment (or meet other conditions), and fulfill certain notification obligations. (Arts. 38, 41). • China can restrict data transfers to overseas individuals or organizations whose personal data processing activities China deems harmful to its interests (Art. 42). • China can also impose reciprocal data transfer restrictions vis-à-vis countries that restrict transfers to China (Art. 43).	Yes. • Critical Information Infrastructure (CII)operators must store personal data and important data in China. If strictly necessary, CII operators may seek an exception from this rule based on an official approval for such transfer following a data security assessment conducted by government authorities. (Art. 30). • All other data handlers must store "important data" in China, subject to official security management procedures for the export of data. (Art. 30).	Yes. • Operators (e.g., automotive OEMs, etc.) must store personal data and important data in China. If strictly necessary, the operator may seek an exception from this rule based on an official approval for such transfer following a cross-border transfer security assessment conducted by government authorities. (ADMR, Art. 12) • Operators are subject to strict legal obligations in connection with any transfer (supervising foreign data recipients; legal liability; data type, scope, use, and process limitations; governmental reporting requirements, etc.) (ADMR, Arts. 13-19) • Strict prohibition of any cross-border transfer of Data relating to roads, buildings, topography, traffic participants, among others, and the vehicle location and track data, collected by a connected vehicle from the environment outside the vehicles through cameras, radar and other sensors (CVSDR, Art. 7.1)

Colombia

Title	Types of Data Covered	Selected Rules in Colombia on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Statutory Law 1266 of 2008 (Law 1266) regulates the processing of financial data, credit records and commercial information collected in Colombia or abroad. Law 1266 defines general terms and establishes basic data processing principles, data subject rights, data controller obligations and specific rules for financial data. Per Law 1581, cross-border data transfers are prohibited unless the country where the data will be transferred to provides at least equivalent data privacy and protection standards and adequate safeguards to those provided by Colombian law. In this regard, adequate levels of data protection will be determined in accordance with the standards set by the SIC. This restriction does not apply in the following cases: • If the Data Subject expressly consented to the cross-border transfer of data • Exchange of medical data • Bank or stock transfers • Transfers agreed to under international treaties to which the Colombia is a party • Transfers necessary for the performance of a contract between the Data Subject and the controller, or for the implementation of pre-contractual measures, provided the data owner consented, and • Transfers legally required in order to safeguard the public interest Therefore, the data controller requires the authorization of the Data Subject for transferring the personal data abroad, unless such transfer is to one of the following countries which, according to the SIC, meet the standard of data protection and security levels. Colombia maintains a list of countries to which transfers are authorized – namely: Albania, Argentina, Austria, Belgium, Bulgaria, Canada, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Perú, Poland, Portugal, Republic of Korea, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, United States, United Kingdom, Uruguay. Colombia also considers that personal data can be transferred to any country regarding which the European Commission considers to meets its standard for levels of protection. The transfer of personal data takes place when the data controller provides personal data to a data processor, in Colombia or abroad, in order to allow the data processor to process the personal data on behalf of the data controller. The data subject's consent is required for the transfer of data, unless an adequate data transfer agreement between the data processor and the data controller is in place. In this regard, Decree 1377 requires that the aforementioned agreement include the following clauses: 1. The extent and limitations of the data treatment 2. The activities that the data processor will perform on behalf of the data controller, and 3. The obligations the data processor has to data subjects and the data controller The data processor has three additional obligations when processing personal data: • Process data according to the legal principles established in Colombian law • Guarantee the safety and security of the databases • Maintain strict confidentiality of the personal data A data controller transferring data to a data processor must identify the data processor in the National Database Register for each database transferred. Finally, the data processor must process the personal data in accordance with the data controller's privacy policy and the authorization given by the data subject.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=CO
General Law on the Protection of Personal Data, Law	Personal	Excerpt (Machine translation): **TITLE VIII - TRANSFER OF DATA TO THIRD COUNTRIES**	Colombia, General Law on the Protection of Personal Data

1581 of 2012 (published in Official Gazette No. 48587 of October 18, 2012)		**Article 26**. Prohibition. The transfer of personal data of any kind to countries that do not provide adequate levels of data protection is prohibited. It is understood that a country offers an adequate level of data protection when it complies with the standards set by the Superintendence of Industry and Commerce on the matter, which in no case may be lower than those required by this law to its recipients. This prohibition shall not apply in the case of: a) Information in respect of which the Holder has granted his express and unequivocal authorization for the transfer; b) Exchange of medical data, when required by the Treatment of the Holder for reasons of health or public hygiene; (c) Bank or stock exchange transfers, in accordance with the legislation applicable to them; (d) Transfers agreed within the framework of international treaties to which the Republic of Colombia is a party, based on the principle of reciprocity; (e) Transfers necessary for the execution of a contract between the Owner and the Data Controller, or for the execution of pre-contractual measures as long as you have the authorization of the Owner; (f) Transfers legally required for the safeguarding of the public interest, or for the recognition, exercise or defence of a right in a judicial proceeding. Paragraph 1. In cases not contemplated as an exception in this article, it will be up to the Superintendence of Industry and Commerce to issue the declaration of conformity regarding the international transfer of personal data. For this purpose, the Superintendent is empowered to request information and advance the proceedings aimed at establishing compliance with the budgets required by the viability of the operation. Paragraph 2. The provisions contained in this article will be applicable to all personal data, including those contemplated in Law 1266 of 2008. **TITLE IX - OTHER PROVISIONS** **Article 27**. Binding Corporate Rules. The National Government will issue the corresponding regulations on Binding Corporate Rules for the certification of good practices in the protection of personal data and its transfer to third countries.	
Decree 1377 of 2013 (June 27, 2013) Partially implementing Law 1581 of 2012	Personal	Excerpt (Machine Translation): CONSIDERATIONS:… That in order to facilitate the implementation and compliance with Law 1581 of 2012, it is necessary to regulate: Matters relating to the authorization of the Information Holder for the processing of their personal data; the treatment of the controllers and processors; the exercise of the rights of the Information Holders; and transfers of personal data and the responsibility demonstrated towards the processing of personal data, the latter issue referring to accountability. … That by virtue of the foregoing: DECREES… CHAPTER I General Provisions Article 3 - Definitions 4. Transfer: The transfer of data takes place when the controller and/or processor of personal data, located in Colombia, sends the information or personal data to a recipient, who in turn is responsible for the treatment, and is located inside or outside the country. CHAPTER V - International transfers and transmissions of personal data Article 24. On the transfer and international transmission of personal data. For the transmission and transfer of personal data, the following rules shall apply: 1. International transfers of personal data must comply with the provisions of Article 26 of Law 1581 of 2012. 2. International transmissions of personal data that are made between a controller and a processor to allow the processor to carry out the processing on behalf of the controller, will not require to be informed to the Holder or have his consent when there is a contract in the terms of article 25 below. Article 25. Contract for the transmission of personal data. The contract signed by the controller with those managing the processing of personal data under their control and responsibility will indicate the scope of the treatment, the activities that the person in charge will carry out on behalf of the person in charge for the processing of personal data and the obligations of the Processor to the owner and the person in charge.	Colombia, Decree 1377 of 2013

		By means of this contract, the person in charge will undertake to apply the obligations of the person in charge under the information processing policy set by it and to carry out the data processing in accordance with the purpose that the Holders have authorized and with the applicable laws. In addition to the obligations imposed by the applicable rules within the aforementioned contract, the following obligations must be included for the lead respective processor: 1. Afford treatment, on behalf of the controller, to personal data in accordance with principles that protect them. 2. Safeguard the security of databases containing personal data. 3. Keep confidentiality regarding the processing of personal data.	

Congo

Title	Types of Data Covered	Selected Rules in Congo on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The protection of personal data is included in the law on telecommunications, information and communication technology N° 20/017 of 25 November 2020 and published in the official journal on 22 September 2021 (the "Law"). The Law entered into force on the date of its approval (25 November 2020). The Ministerial Decree which should regulate the more practical details of the law has not yet been issued. Explicit and prior consent of the data subject is required to transfer that person's data to another jurisdiction.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=CD
Loi n° 29-2019 du 10 octobre 2019 portant protection des données à caractère personnel	Personal	Not excerpted or summarized due to lack of translation.	https://www.sgg.cg/JO/2019/congo-jo-2019-45.pdf

Costa Rica

Title	Types of Data Covered	Selected Rules in Costa Rica on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Data privacy regulation in Costa Rica is contained in two laws: Law No. 7975, the Undisclosed Information Law, which makes it a crime to disclose confidential and/or personal information without authorization; and Law No. 8968, Protection in the Handling of the Personal Data of Individuals together with its by-laws, which were enacted to regulate the activities of companies that administer databases containing personal information. The transfer of personal information is authorized by the Laws if the data subject provides prior, unequivocal, express and valid written consent to the company that manages the database. Such transfers cannot violate the principles and rights granted in the Laws. Also, there are specific limitations regarding cross-border transfers of personal information. The transfer of personal information from the person responsible for a database to a service supplier, technological intermediary, or entities in the same economic interest group is not considered a transfer of personal information and thus does not need authorization from the data subject. Also, the transfer of public information (which can be generally accessed) does not need authorization from the data subject.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=CR
Regulations to the Law for the Protection of the Person against the Treatment of their Personal Data No. 37554-JP	Personal	Excerpt **Article 2.** Definitions, abbreviations and acronyms w) Transfer of personal data: Action through which personal data of the person responsible for a personal database is transferred to any third party other than the person responsible, its economic interest group, the person in charge, service provider or technological intermediary, in these cases as long as the recipient does not use the data for distribution, dissemination or marketing. **Chapter V - Transfer of Personal Data** **Article 40.** Conditions for the transfer. The transfer will always require the unequivocal consent of the holder. The transfer implies the transfer of personal data by, solely and exclusively, the person in charge who transfers to the person in charge who receives the personal data. Said transfer of personal data will always require the informed consent of the owner, unless otherwise provided by law, as well as that the data to be transferred have been collected or collected in a lawful manner and according to the criteria established by the Law and these Regulations. The transfer of personal data from the person responsible for a database to a manager, service provider or technological intermediary or the companies of the same economic interest group is not considered a transfer. Any sale of data from the file or from the database, partial or total, must meet the requirements established in the previous paragraph. (As amended by Article 8 of Executive Decree No. 40008 of July 19, 2016) **Article 41**. Compliance with the minimum action protocols . The transfers of personal data by those responsible will be subject to faithful compliance with the minimum action protocols, duly registered with the Agency. **Article 42**. Burden of proof . For the purposes of demonstrating that the transfer of personal data was carried out in accordance with the Law and these Regulations, the burden of proof will fall on the person responsible. **Article 43**. Contract for data transfer . The person responsible for the transfer of personal data must establish a contract with the receiving person in charge, which foresees at least the same obligations to which the person responsible for the transfer of said data is subject. **Chapter VII -** Of the Protection of Rights before the Agency	http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=74352

Title	Types of Data Covered	Selected Rules in Costa Rica on Cross-Border Data Transfers or Data Localization	Sources
		Article 58. Start of the Rights Protection procedure . Any person who has a subjective right or a legitimate interest can report to the Agency that a public or private database acts in contravention of the rules or basic principles for data protection and information self-determination, established by the Law and this Regulation. Likewise, the Agency may ex officio initiate a procedure aimed at verifying whether a database is being used or not, in accordance with the Law and this Regulation. The Agency in processing the data protection procedure, will apply the principles established in the Second Book of the General Law of Public Administration. **Article 59**. Causes . The rights protection procedure will proceed when: a. Personal data is collected for use in the database without sufficient and extensive information being given to the person concerned; b. Personal data is collected, stored and transmitted through insecure mechanisms or that in some way do not guarantee the security and inalterability of the data; c. Personal data is collected, stored, transmitted or otherwise used without the informed and express consent of the data owner; d. Personal data is transferred to other people or companies in contravention of the rules established in the Law and this Regulation; e. Personal data is collected, stored, transmitted or otherwise used for a purpose other than that authorized by the owner of the information; f. Unjustifiably refuses to give a holder access to the data contained in files and databases, in order to verify its quality, collection, storage and use in accordance with the Law and this Regulation; g. Unjustifiably refuses to delete or rectify the data of a person who has requested it by clear and unequivocal means; h. Sensitive data is collected, stored, transmitted or in any other way used, by private individuals or legal entities, without the consent of its owner or without a law or special regulation that authorizes it; i. Personal data is obtained from the owners or third parties by means of deception, violence, fraud, bad faith or threat; j. Information registered in a personal database whose secrecy is required to be kept in accordance with the Law is revealed: k. False or different information contained in a data file is provided to a third party, knowingly; l. Processing of personal data is carried out without being duly registered with the Agency; m. Personal information of Costa Ricans or foreigners residing in the country is transferred to the databases of third countries, without the consent of their owners. n. For other reasons that, in the opinion of the Agency, affect the rights of the owner in accordance with the Law and these Regulations.	
Ley de protección de la persona frente al tratamiento de sus datos personales - Ley n.º 8968	Personal	Not excerpted or summarized due to lack of translation.	OEA :: SAJ :: Departamento de Derecho Internacional (DDI):: Protección de Datos Personales (oas.org)

Côte d'Ivoire

Title	Types of Data Covered	Selected Rules in Côte d'Ivoire on Cross-Border Data Transfers or Data Localization	Sources
Loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel (in French)	Personal	Not excerpted or summarized due to lack of translation.	http://media.mofo.com/files/PrivacyLibrary/3979/Cote-d-voire-loi_2013_450.pdf

Croatia

Title	Types of Data Covered	Selected Rules in Croatia on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	See Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Cyprus

Title	Types of Data Covered	Selected Rules in Cyprus on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Czech Republic

Title	Types of Data Covered	Selected Rules in Czech Republic on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Denmark

Title	Types of Data Covered	Selected Rules in Denmark on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Dominican Republic

Title	Types of Data Covered	Selected Rules in Dominican Republic on Cross-Border Data Transfers or Data Localization	Sources
Ley No. 172-13, sobre Protección de Datos de Carácter Personal del 13 de diciembre de 2013	Personal data	Not excerpted or summarized due to lack of translation.	https://poderjudicial.gob.do/documentos/PDF/leyes/LEY_172_13.pdf

Ecuador

Title	Types of Data Covered	Selected Rules in Ecuador on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Since May 26, 2021, Ecuador adopted the Personal Data Protection Organic Law, whose main purpose is to guarantee the right to the protection of personal data, that includes the access and decision on information and personal data, as well as its corresponding protection. Under the law, personal data may be transferred or communicated to third parties when it is carried out for the fulfillment of purposes directly related to the legitimate functions of the controller and the recipient, when the transfer is configured within one of the grounds of legitimacy and also has the consent of the owner. It shall be understood that the consent is informed when for the transfer or communication of personal data the data controller has provided sufficient information to the data subject to enable him/her to know the purpose for which his/her data will be used and the type of activity of the third party to whom it is intended to transfer or communicate such data. It will not be considered a transfer or communication in the event that the processor or a third-party accesses personal data for the provision of a service to the controller of personal data. The third party who has legitimately accessed personal data in these considerations shall be considered the processor. The treatment of personal data carried out by the processor or by a third party must be regulated by a contract, in which it is clearly and precisely established that the personal data processor or the third party will only process the information in accordance with the instructions of the owner and will not use it for purposes other than those indicated in the contract, nor transfer or communicate it even for storage to other persons. Once the contractual performance has been fulfilled, the personal data shall be destroyed or returned to the data controller under the supervision of the Personal Data Protection Authority. The processor or third party shall be liable for any infringements arising from non-compliance with the conditions of personal data processing set forth in this Law.	https://www.dlapiperdataprotection.com/index.html?t=law&c=EC
Protection of Privacy and Personal Data Organic Law 2019	Personal data	Not excerpted or summarized due to lack of translation.	https://www.nmslaw.com.ec/wp-content/uploads/2019/09/Proyecto-de-Ley-Org%C3%A1nica-de-Protecci%C3%B3n-de-Datos-Personales.pdf

Egypt

Title	Types of Data Covered	Selected Rules in Egypt on Cross-Border Data Transfers or Data Localization	Sources
Law on the Protection of Personal Data (July 15, 2020) (Resolution No. 151 of 2020)	Personal	Summary: Cross border transfers: Subject to a number of exceptions, the Law contains a general prohibition on the transfer of personal data (including sharing and storing of personal data) to a foreign country unless a licence has been obtained from the Centre and where the level of protection is not less than that provided under the Law. The Law, however, does not provide a list of "adequate regimes" unlike other data protection laws; as such, it is not clear how the level of protection would be determined. Further criteria, policies and regulations for cross border transfers are intended to be specified in the Executive Regulations. Licensing Requirements: Controllers and Processors have to obtain a license or permit from the Centre to conduct cross-border transfers of personal data (among other things). A maximum fee payable for a license shall be 2,000,000 Egyptian Pounds (approximately US$125,000). However, exceptions are made under Article (15) of the Law, if the direct consent of the data subject or his representative is obtained for transferring, sharing, circulating or processing personal data to a country that does not offer the same level of protection in the following cases: • To protect the data subject's life and provide them with medical care, treatment, or the administration of medical services. • To perform obligations in order to prove the existence of a legal right or to exercise or defend such right before the judiciary. • To conclude or perform an agreement entered into by the person responsible for processing the personal data and third party, which shall be in favor of the concerned data subject. • To perform a procedure required under an international judicial cooperation. • There is legal necessity or obligation to protect the public interest. • To transfer money to another country pursuant to the laws in force of that country. • If the transfer or circulation is pursuant to a bilateral or multilateral agreement, to which the Arab Republic of Egypt is a party. In addition, the controller or the processor may, as the case may be, grant access to personal data to another controller or processor outside the Arab Republic of Egypt by virtue of a license from the Centre provided that the following conditions have been met: • There is conformity between the nature of work of either of the controllers or processors, or unity between the purposes for which they obtain the personal data. • Either the controllers or processors, or the data subject, have a legitimate interest in the personal data. The level of legal and technical protection of the personal data offered by the controller or the processor abroad shall not fall below the level of protection provided in the Arab Republic of Egypt. Sanctions: The Centre can impose significant fines and/or criminal sanctions for breaches of the Law, such as: a maximum of 5,000,000 Egyptian Pounds (approximately US$310,000) and/or imprisonment of up to three years on: (i) any Data Holder, Data Controller or Data Processor for collecting, processing, storing sensitive personal data without a licence; or (ii) each person who transfers data outside of Egypt without a licence or a permit.	Egypt, Law on the Protection of Personal Data Clyde & Co., Egypt's Data Protection Law enters into force OneTrust: Egypt Summary DLA: https://www.dlapiperdataprotection.com/index.html?t=transfer&c=EG

El Salvador

Title	Types of Data Covered	Selected Rules in El Salvador on Cross-Border Data Transfers or Data Localization	Sources
Bill - Ley de Comercio Electronico y Comunicaciones	Personal	Not excerpted or summarized due to lack of translation.	https://www.asamblea.gob.sv/sites/default/files/documents/correspondencia/2A326CE8-F13A-4828-8640-648235C228BF.pdf

Estonia

Title	Types of Data Covered	Selected Rules in Estonia on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

European Union

Title	Types of Data Covered	Selected Rules in European Union on Cross-Border Data Transfers or Data Localization	Sources
		The EU cross-border data provisions outlined in this table include the following: (1) General Data Protection Regulation (GDPR), (2) EU Data Governance Act, (3) EU Data Act Proposal, and (4) EU Health Data Space Proposal. The summary below addresses the GDPR only. "Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44). The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand. Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on the condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities. The GDPR also includes a list of context specific derogations, permitting transfers to third countries where: a. explicit informed consent has been obtained; b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures; c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person; d. the transfer is necessary for important reasons of public interest; e. the transfer is necessary for the establishment, exercise or defence of legal claims; f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions. There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation. Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR. The exchange of personal data with the diplomatic representations of foreign governments or international institutions in the Republic of Albania shall be considered an international transfer of data."" Following the so-called Schrems II decision, which invalidated the US-EU Privacy Shield data transfer framework, European authorities have adopted several related follow-on measures that increase the restrictiveness of the EU's cross-border data policy framework. This includes the adoption of a new Standard Contractual Clause imposing new obligations to assess the risk of data transfers to third countries.	Transfer in the EU - DLA Piper Global Data Protection Laws of the World (dlapiperdataprotection.com)

Title	Types of Data Covered	Selected Rules in European Union on Cross-Border Data Transfers or Data Localization	Sources
		Based on the Schrems II ruling, several EU Member State Data Protection Authorities have begun issuing statements or rulings opining on the legality of data transfers to the United States using certain digital productivity tools. These decisions include the following: • Spain (December 15, 2022 decision) • Denmark (September 21 decision; September 8 Aarhus decision; August 8 Helsingør decision; July 2022 statement, Jan. 2022 statement) • Austria (Oct. 2021, April 2022), • Germany (Berlin DPA) • France (CNIL ruling) • Guernsey (DPA ruling) • Italy (Garante June 23 ruling), and • The Netherlands (Dutch DPA statement).	
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)	Personal	Excerpt **CHAPTER V** - Transfers of personal data to third countries or international organisations **Article 44** - General principle for transfers Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined. **Article 45** Transfers on the basis of an adequacy decision 1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation. 2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements: (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred; (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data. 3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Title	Types of Data Covered	Selected Rules in European Union on Cross-Border Data Transfers or Data Localization	Sources
		organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2). 4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC. 5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2). On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3). 6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5 7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49. 8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured. 9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article. **Article 46** - Transfers subject to appropriate safeguards 1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. 2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: (a) a legally binding and enforceable instrument between public authorities or bodies; (b) binding corporate rules in accordance with Article 47; (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2); (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2); (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. 3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by: (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights. 4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article. 5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article **Article 47** - Binding corporate rules 1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:	

Title	Types of Data Covered	Selected Rules in European Union on Cross-Border Data Transfers or Data Localization	Sources
		(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees; (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and (c) fulfil the requirements laid down in paragraph 2. 2. The binding corporate rules referred to in paragraph 1 shall specify at least: (a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members; (b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question; (c) their legally binding nature, both internally and externally; (d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules; (e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules; (f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage; (g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14; (h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling; (i) the complaint procedures; (j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority; (k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory (l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j); (m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and (n) the appropriate data protection training to personnel having permanent or regular access to personal data. 3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2). **Article 48** - Transfers or disclosures not authorised by Union law Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter. **Article 49** - Derogations for specific situations 1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:	

Title	Types of Data Covered	Selected Rules in European Union on Cross-Border Data Transfers or Data Localization	Sources
		(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; (d) the transfer is necessary for important reasons of public interest; (e) the transfer is necessary for the establishment, exercise or defence of legal claims; (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case. Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued. 2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients. 3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers. 4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject. 5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission. 6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30. **Article 50** - International cooperation for the protection of personal data In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to: (a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data; (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms; (c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; (d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.	

Title	Types of Data Covered	Selected Rules in European Union on Cross-Border Data Transfers or Data Localization	Sources
		CHAPTER VII ***International access and transfer*** *Article 31* **International access and transfer** 1. The public sector body, the natural or legal person to which the right to re-use data was granted under Chapter II, the data intermediation services provider or the recognised data altruism organisation shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3. 2. Any decision or judgment of a third-country court or tribunal and any decision of a third-country administrative authority requiring a public sector body, a natural or legal person to which the right to re-use data was granted under Chapter II, a data intermediation services provider or recognised data altruism organisation to transfer or give access to non-personal data within the scope of this Regulation held in the Union shall be recognised or enforceable in any manner only if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or any such agreement between the requesting third country and a Member State. 3. In the absence of an international agreement as referred to in paragraph 2 of this Article, where a public sector body, a natural or legal person to which the right to re-use data was granted under Chapter II, a data intermediation services provider or recognised data altruism organisation is the addressee of a decision or judgment of a third-country court or tribunal or a decision of a third-country administrative authority to transfer or give access to non-personal data within the scope of this Regulation held in the Union and compliance with such a decision would risk putting the addressee in conflict with Union law or with the national law of the relevant Member State, transfer to or access to such data by that third-country authority shall take place only where: (a) the third-country system requires the reasons and proportionality of such a decision or judgment to be set out and requires such a decision or judgment to be specific in character, for instance by establishing a sufficient link to certain suspected persons or infringements; (b) the reasoned objection of the addressee is subject to a review by a competent third-country court or tribunal; and (c) the competent third-country court or tribunal issuing the decision or judgment or reviewing the decision of an administrative authority is empowered under the law of that third country to take duly into account the relevant legal interests of the provider of the data protected under Union law or the national law of the relevant Member State. 4. If the conditions laid down in paragraph 2 or 3 are met, the public sector body, the natural or legal person to which the right to re-use data was granted under Chapter II, the data intermediation services provider or the recognised data altruism organisation shall provide the minimum amount of data permissible in response to a request, based on a reasonable interpretation of the request. 5. The public sector body, the natural or legal person to which the right to re-use data was granted under Chapter II, the data intermediation services provider and the recognised data altruism organisation shall inform the data holder about the existence of a request of a third-country administrative authority to access its data before complying with that request, except where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity. **Relevant Paragraphs from Preamble** (20) In order to preserve fair competition and the open market economy it is of the utmost importance to safeguard protected data of non-personal nature, in particular trade secrets, but also non-personal data representing content protected by intellectual property rights from unlawful access that may lead to intellectual property theft or industrial espionage. In order to ensure the protection of the rights or interests of data holders, it should be possible to transfer non-personal data which is to be protected from unlawful or unauthorised access in accordance with Union or national law and which is held by public sector bodies to third countries, but only where appropriate safeguards for the use of data are provided. Such appropriate safeguards should include a requirement that the public sector body transmit protected data to a re-user only if that re-user makes contractual commitments in the interest of the protection of the data. A re-user that intends to transfer the protected data to a third country	

Title	Types of Data Covered	Selected Rules in European Union on Cross-Border Data Transfers or Data Localization	Sources
		should comply with the obligations laid down in this Regulation even after the data has been transferred to the third country. To ensure the proper enforcement of such obligations, the re-user should also accept the jurisdiction of the Member State of the public sector body that allowed the re-use for the judicial settlement of disputes. (21) Appropriate safeguards should also be considered to be implemented where, in the third country to which non-personal data is being transferred, there are equivalent measures in place which ensure that data benefit from a level of protection similar to that applicable by means of Union law, in particular with regard to the protection of trade secrets and intellectual property rights. To that end, the Commission should be able to declare, by means of implementing acts, where justified because of the substantial number of requests across the Union concerning the re-use of non-personal data in specific third countries, that a third country provides a level of protection that is essentially equivalent to that provided by Union law. The Commission should assess the necessity of such implementing acts on the basis of information provided by the Member States through the European Data Innovation Board. Such implementing acts would reassure public sector bodies that re-use of data held by public sector bodies in the third country concerned would not compromise the protected nature of that data. The assessment of the level of protection afforded in the third country concerned should, in particular, take into consideration the relevant general and sectoral law, including on public security, defence, national security and criminal law, concerning access to and protection of non-personal data, any access by the public sector bodies of that third country to the data transferred, the existence and effective functioning of one or more independent supervisory authorities in the third country with responsibility for ensuring and enforcing compliance with the legal regime ensuring access to such data, the third country's international commitments regarding the protection of data, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems. The existence of effective legal remedies for data holders, public sector bodies or data intermediation services providers in the third country concerned is of particular importance in the context of the transfer of non-personal data to that third country. Such safeguards should therefore include the availability of enforceable rights and of effective legal remedies. Such implementing acts should be without prejudice to any legal obligation or contractual arrangements already undertaken by a re-user in the interest of the protection of non-personal data, in particular industrial data, and to the right of public sector bodies to oblige re-users to comply with conditions for re-use, in accordance with this Regulation. (22) Some third countries adopt laws, regulations and other legal acts which aim to directly transfer or provide governmental access to non-personal data in the Union under the control of natural and legal persons under the jurisdiction of the Member States. Decisions and judgments of third-country courts or tribunals or decisions of third-country administrative authorities requiring such transfer of or access to non-personal data should be enforceable where they are based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. In some cases, situations may arise where the obligation to transfer or provide access to non-personal data arising from a third country law conflicts with a competing obligation to protect such data under Union or national law, in particular with regard to the protection of the fundamental rights of the individual or of the fundamental interests of a Member State related to national security or defence, as well as the protection of commercially sensitive data and the protection of intellectual property rights, including contractual undertakings regarding confidentiality in accordance with such law. In the absence of international agreements regulating such matters, the transfer of or access to non-personal data should be allowed only if, in particular, it has been verified that the third-country's legal system requires the reasons and proportionality of the decision or judgment to be set out, that the decision or judgment is specific in character, and that the reasoned objection of the addressee is subject to a review by a competent third-country court or tribunal, which is empowered to take duly into account the relevant legal interests of the provider of such data. Moreover, public sector bodies, natural or legal persons to which the right to re-use data was granted, data intermediation services providers and recognised data altruism organisations should ensure, where they sign contractual agreements with other private parties, that non-personal data held in the Union are accessed in or transferred to third countries only in accordance with Union law or the national law of the relevant Member State. (23) To foster further trust in the data economy of the Union, it is essential that the safeguards in relation to Union citizens, the public sector and undertakings that ensure control over their strategic and sensitive data are implemented and that Union law, values and standards are upheld in terms of, but not limited to, security, data protection and consumer protection. In order to prevent unlawful access to non-personal data, public sector bodies, natural or legal persons to which the right to re-use data was granted, data intermediation services providers and recognised data altruism organisations should take all reasonable measures to prevent access to the systems where non-personal data is stored, including encryption of data or corporate policies. To that end, it should be ensured that public sector bodies, natural or legal persons to which the right to re-use data was granted, data intermediation services providers and recognised data altruism organisations adhere to all relevant technical standards, codes of conduct and certifications at Union level. (24) In order to build trust in re-use mechanisms, it may be necessary to attach stricter conditions for certain types of non-personal data that may be identified as highly sensitive in future specific Union legislative acts, with regard to the transfer to third countries, if such transfer could jeopardise Union public policy objectives, in line with international commitments. For example, in the health domain, certain datasets held by actors in the public health system, such as public hospitals, could be identified as highly sensitive health data. Other relevant sectors include transport, energy, environment and finance. In order to ensure harmonised practices across the Union, such types of highly sensitive non-personal public data should be defined by Union law, for example in the context of the European health data space or other sectoral law.	

Title	Types of Data Covered	Selected Rules in European Union on Cross-Border Data Transfers or Data Localization	Sources
		Those conditions attached to the transfer of such data to third countries should be laid down in delegated acts. Conditions should be proportionate, non-discriminatory and necessary to protect legitimate Union public policy objectives identified, such as the protection of public health, safety, the environment, public morality, consumer protection, privacy and personal data protection. The conditions should correspond to the risks identified in relation to the sensitivity of such data, including in terms of the risk of the re-identification of individuals. Such conditions could include terms applicable for the transfer or technical arrangements, such as the requirement to use a secure processing environment, limitations with regard to the re-use of data in third countries or categories of persons entitled to transfer such data to third countries or to access the data in the third country. In exceptional cases such conditions could also include restrictions to the transfer of the data to third countries to protect the public interest.	
Proposal for a Regulation of the European Parliament and the Council on Harmonised Rules and Fair Access to Data (Data Act), COM 2022/68/Final (Feb. 23, 2022)	Non-Personal Data	**EU Data Act Proposal, Chapter VII – International Contexts – Non-Personal Data Safeguards** Article 27 International access and transfer 1. Providers of data processing services shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3. 2. Any decision or judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a provider of data processing services to transfer from or give access to non-personal data within the scope of this Regulation held in the Union may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or any such agreement between the requesting third country and a Member State. 3. In the absence of such an international agreement, where a provider of data processing services is the addressee of a decision of a court or a tribunal or a decision of an administrative authority of a third country to transfer from or give access to non-personal data within the scope of this Regulation held in the Union and compliance with such a decision would risk putting the addressee in conflict with Union law or with the national law of the relevant Member State, transfer to or access to such data by that third-country authority shall take place only: (a) where the third-country system requires the reasons and proportionality of the decision or judgement to be set out, and it requires such decision or judgement, as the case may be, to be specific in character, for instance by establishing a sufficient link to certain suspected persons, or infringements; (b) the reasoned objection of the addressee is subject to a review by a competent court or tribunal in the third-country; and (c) the competent court or tribunal issuing the decision or judgement or reviewing the decision of an administrative authority is empowered under the law of that country to take duly into account the relevant legal interests of the provider of the data protected by Union law or national law of the relevant Member State. The addressee of the decision may ask the opinion of the relevant competent bodies or authorities, pursuant to this Regulation, in order to determine whether these conditions are met, notably when it considers that the decision may relate to commercially sensitive data, or may impinge on national security or defence interests of the Union or its Member States. The European Data Innovation Board established under Regulation [xxx – DGA] shall advise and assist the Commission in developing guidelines on the assessment of whether these conditions are met. 4. If the conditions in paragraph 2 or 3 are met, the provider of data processing services shall provide the minimum amount of data permissible in response to a request, based on a reasonable interpretation thereof. 5. The provider of data processing services shall inform the data holder about the existence of a request of an administrative authority in a third-country to access its data before complying with its request, except in cases where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity. "Specific Objectives" include... "Put in place safeguards against unlawful data transfer without notification by cloud service providers. This is because concerns have been raised about non-EU/European Economic Area (EEA) governments' unlawful access to data. Such safeguards should further enhance trust in the data processing services that increasingly underpin the European data economy." Paragraph 77 of Preambular Clauses: "Third countries may adopt laws, regulations and other legal acts that aim at directly transferring or providing governmental access to non-personal data located outside their borders, including in the Union. Judgments of courts or tribunals or decisions of other judicial or administrative authorities, including law	EU Data Act, EUR-Lex - 52022PC0068 - EN - EUR-Lex (europa.eu), at : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN; *See also,* A European Strategy for data | Shaping Europe's digital future (europa.eu)

Title	Types of Data Covered	Selected Rules in European Union on Cross-Border Data Transfers or Data Localization	Sources
		enforcement authorities in third countries requiring such transfer or access to non-personal data should be enforceable when based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. In other cases, situations may arise where a request to transfer or provide access to non-personal data arising from a third country law conflicts with an obligation to protect such data under Union law or national law, in particular as regards the protection of fundamental rights of the individual, such as the right to security and the right to effective remedy, or the fundamental interests of a Member State related to national security or defence, as well as the protection of commercially sensitive data, including the protection of trade secrets, and the protection of intellectual property rights, and including its contractual undertakings regarding confidentiality in accordance with such law. In the absence of international agreements regulating such matters, transfer or access should only be allowed if it has been verified that the third country's legal system requires the reasons and proportionality of the decision to be set out, that the court order or the decision is specific in character, and that the reasoned objection of the addressee is subject to a review by a competent court in the third country, which is empowered to take duly into account the relevant legal interests of the provider of such data. Wherever possible under the terms of the data access request of the third country's authority, the provider of data processing services should be able to inform the customer whose data are being requested in order to verify the presence of a potential conflict of such access with Union or national rules, such as those on the protection of commercially sensitive data, including the protection of trade secrets and intellectual property rights and the contractual undertakings regarding confidentiality."	
Proposal for a Regulation of the European Parliament and the Council on the European Health Data Space, COM 2022/197 (May 3, 2022)	Health-related data	**Proposal for a European Health Data Space,** Articles 9 and 61-63 Article 9 Identification management 1. Where a natural person uses telemedicine services or personal health data access services referred to in Article 3(5), point (a), that natural person shall have the right to identify electronically using any electronic identification means which is recognised pursuant to Article 6 of Regulation (EU) No 910/2014. 2. The Commission shall, by means of implementing acts, determine the requirements for the interoperable, cross-border identification and authentication mechanism for natural persons and health professionals, in accordance with Regulation (EU) No 910/2014 as amended by [COM(2021) 281 final]. The mechanism shall facilitate the transferability of electronic health data in a cross-border context. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 68(2). 3. The Commission shall implement services required by the interoperable, cross-border identification and authentication mechanism referred to in paragraph 2 of this Article at Union level, as part of the cross-border digital health infrastructure referred to in Article 12(3). 4. The digital health authorities and the Commission shall implement the cross-border identification and authentication mechanism at Union and Member States' level, respectively. Article 61 Third country transfer of non-personal electronic data 1. Non-personal electronic data made available by health data access bodies, that are based on a natural person's electronic data falling within one of the categories of Article 33 [(a), (e), (f), (i), (j), (k), (m)] shall be deemed highly sensitive within the meaning of Article 5(13) of Regulation […] [Data Governance Act COM/2020/767 final], provided that their transfer to third countries presents a risk of re-identification through means going beyond those likely reasonably to be used, in view of the limited number of natural persons involved in that data, the fact that they are geographically scattered or the technological developments expected in the near future. 2. The protective measures for the categories of data mentioned in paragraph 1 shall depend on the nature of the data and anonymization techniques and shall be detailed in the Delegated Act under the empowerment set out in Article 5(13) of Regulation […] [Data Governance Act COM/2020/767 final]. Article 62 International access and transfer of non-personal electronic health data 1. The digital health authorities, health data access bodies, the authorised participants in the cross-border infrastructures provided for in Articles 12 and 52 and data users shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal electronic health data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3 of this Article. 2. Any judgment of a third-country court or tribunal and any decision of a third-country administrative authority requiring a digital health authority, health data access body or data users to transfer or give access to non-personal electronic health data within the scope of this Regulation held in the Union shall be recognised or enforceable in any manner only if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or any such agreement between the requesting third country and a Member State.	Proposal for a Regulation of the European Parliament and the Council on the European Health Data Space, https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=CELEX:52022PC0197&from=EN *See also,* European Health Data Space (europa.eu)

Title	Types of Data Covered	Selected Rules in European Union on Cross-Border Data Transfers or Data Localization	Sources
		3. In the absence of an international agreement as referred to in paragraph 2 of this Article, where a digital health authority, a health data access body, data users is the addressee of a decision or judgment of a third-country court or tribunal or a decision of a third-country administrative authority to transfer or give access to non-personal data within the scope of this Regulation held in the Union and compliance with such a decision would risk putting the addressee in conflict with Union law or with the national law of the relevant Member State, transfer to or access to such data by that third-country authority shall take place only where: (a) the third-country system requires the reasons and proportionality of such a decision or judgment to be set out and requires such a decision or judgment to be specific in character, for instance by establishing a sufficient link to certain suspected persons or infringements; (b) the reasoned objection of the addressee is subject to a review by a competent third-country court or tribunal; and (c) the competent third-country court or tribunal issuing the decision or judgment or reviewing the decision of an administrative authority is empowered under the law of that third country to take duly into account the relevant legal interests of the provider of the data protected under Union law or the national law of the relevant Member State 4. If the conditions laid down in paragraph 2 or 3 are met, digital health authority, a health data access body or a data altruism body shall provide the minimum amount of data permissible in response to a request, based on a reasonable interpretation of the request. 5. The digital health authorities, health data access bodies, data users shall inform the data holder about the existence of a request of a third-country administrative authority to access its data before complying with that request, except where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity. Article 63 International access and transfer of personal electronic health data In the context of international access and transfer of personal electronic health data, Member States may maintain or introduce further conditions, including limitations, in accordance with and under the conditions of article 9(4) of the Regulation (EU) 2016/679. Para. 67 of Preambular Text: Certain categories of electronic health data can remain particularly sensitive even when they are in anonymised format and thus non-personal, as already specifically foreseen in the Data Governance Act. Even in situations of the use of state of the art anonymization techniques, there remains a residual risk that the capacity to re-identify could be or become available, beyond the means reasonably likely to be used. Such residual risk is present in relation to rare diseases (a life-threatening or chronically debilitating condition affecting not more than five in 10 thousand persons in the Union), where the limited numbers of case reduce the possibility to fully aggregate the published data in order to preserve the privacy of natural persons while also maintaining an appropriate level of granularity in order to remain meaningful. It can affect different types of health data depending on the level of granularity and description of the characteristics of data subjects, the number of people affected or and for instance in cases of data included in electronic health records, disease registries, biobanks, person generated data etc. where the identification characteristics are broader and where, in combination with other information (e.g. in very small geographical areas) or through the technological evolution of methods which had not been available at the moment of anonymisation, can lead to the re-identification of the data subjects using means that are beyond those reasonably likely to be used. The realisation of such risk of re-identification of natural persons would present a major concern and is likely to put the acceptance of the policy and rules on secondary use provided for in this Regulation at risk. Furthermore, aggregation techniques are less tested for non-personal data containing for example trade secrets, as in the reporting on clinical trials, and enforcement of breaches of trade secrets outside the Union is more difficult in the absence of a sufficient international protection standard. Therefore, for these types of health data, there remains a risk for re-identification after the anonymisation or aggregation, which could not be reasonably mitigated initially. This falls within the criteria indicated in Article 5(13) of Regulation […] [Data Governance Act COM/2020/767 final]. These types of health data would thus fall within the empowerment set out in Article 5(13) of Regulation […] [Data Governance Act COM/2020/767 final] for transfer to third countries. The protective measures, proportional to the risk of re-identification, would need to take into account the specificities of different data categories or of different anonymization or aggregation techniques and will be detailed in the context of the Delegated Act under the empowerment set out in Article 5(13) of Regulation […] [Data Governance Act COM/2020/767 final].	

Finland

Title	Types of Data Covered	Selected Rules in Finland on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

France

Title	Types of Data Covered	Selected Rules in France on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Title	Types of Data Covered	Selected Rules in Gabon on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The data protection regime in Gabon is governed by the following laws and regulations: • Law No. 001/2011 on the Protection of Personal Data “the Law”; • Law No. 26/2018 of 22 October 2018 regarding Electronic Communications in Gabon; • Law No. 02/2004 of 30 March 2005 ratifying the International Convention for the Suppression of the Financing of Terrorism; • Regulation No. 01/03 -CEMAC-UMAC relating to the Prevention and Suppression of Money Laundering and Financing of Terrorism in Central Africa; • Order n°00000014/PR/2018 of February 23, 2018 on the regulation of electronic transactions in the Gabonese Republic; and • Order No. 15-PR-2018 on the Regulation of Cybersecurity and the Fight against Cybercrime. Data transfers to another country are prohibited unless the other country ensures an adequate level of privacy protection and protection of fundamental rights and freedoms of individuals with regard to the processing operation. The list of countries that comply with this adequate level of protection shall be published by CNPDCP. As far as we are aware, this list has not yet been published. However, the Data Protection Law does identify the criteria which must be considered by the CNPDCP in order to determine adequacy: • the legal provisions existing in the country in question; • the security measures enforced; • the specific circumstances of the processing (such as the purpose and duration thereof); and • the nature, origin, and destination of the data. As an alternative to the 'adequacy' criteria, data controllers may transfer data if: • the data subject has consented expressly to its transfer; • the transfer is necessary to save that person's life; • the transfer is necessary to safeguard a public interest; • the transfer is necessary to ensure the right of defence in a court of law; or • the transfer is necessary for the performance of a contract between the data subject and the data controller, at the request of the data subject, or for the performance of a contract between the data controller and a third party in the interest of the data subject. Except in very specific circumstances, the international transfer of non-encrypted personal data for the purpose of investigation in the health sector is not possible, given the sensitivity of the data at stake. In relation to outsourcing, the Data Protection Law does not provide for specific provisions, except: • the obligations applicable to the relationship with data processors; • when data processors are located outside the country, the provisions applicable to international data transfers; and • general security obligations, which vary depending on the nature of the data at stake (Article 94 and sq. of the Law). No references are included to specific concerns regarding, for example, outsourcing to the cloud or to data centres.	https://www.dlapiperdataprotection.com/index.html?t=law&c=GA
Loi n°001/2011 relative à la protection des données à caractère personnel (in French)	Personal	Not excerpted or summarized due to lack of translation.	https://www.afapdp.org/wp-content/uploads/2012/01/Gabon-Loi-relative-%c3%a0-la-protection-des-donn%c3%a9es-personnelles-du-4-mai-20112.pdf

Georgia

Title	Types of Data Covered	Selected Rules in Georgia on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Under the Law of Georgia On Personal Data Protection (N5669-RS, 28/12/2011) ('**PDP Law**'), Transfer of personal data outside Georgia is admissible without a separate authorisation from the State Inspector if one of the two following conditions apply: • A respective legal ground for data processing exists and the proper standards for the safety of data are secured in the relevant country. The State Inspector has approved the list of such countries; • The processing of data is stipulated under an international agreement between Georgia and the relevant country; However, the general data processing rules will still apply, including securing a necessary legal ground such as the data subject's consent and the requirements of proportionality and necessity. If neither of these conditions apply, then there should be a formal written agreement between the transferor and the data's recipient under which the data's recipient shall commit to ensure proper guarantees to protect the data. In this case, the State Inspector must be presented with such agreement and other relevant information or documents for data transfer approval.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=GE
Law of Georgia on Personal Data Protection	Personal	Excerpt (translated versión) **Chapter VI –** Transfer of Data to Other States and International Organisations **Article 41 –** Data transfer to other states and international organisations 1. Data may be transferred to other states and international organisations if there are grounds for data processing under this Law and if appropriate data protection guarantees are provided by the respective state or international organisation. 2. Data may also be transferred to other states and international organisations, except for paragraph 1 of this article, if: a) the data transfer is part of a treaty or an international agreement of Georgia; b) a data processor provides appropriate guarantees for protection of data and of fundamental rights of a data subject on the basis of an agreement between a data processor and the respective state, a natural or legal person of this state or an international organisation. 3. Data may be transferred under paragraph 2(b) of this article only with permission of the Inspector. **Article 42** – Establishing appropriate guarantees for data protection The Inspector shall assess the presence of appropriate guarantees for data protection in other states and/or international organisations, and make a decision on the basis of analysis of the legislation regulating data processing and the practice. **Article 52** - Violation of rules for data transfer to another state and international organisation 1. Transfer of data in violation of rules established under Article 41 of this Law shall result in a fine of GEL 1 000. 2. The same act committed by a person who has had an administrative penalty imposed in the course of one year for a violation under paragraph 1 of this article shall result in a fine of GEL 3 000. (Law of Georgia No 2639 of 1 August 2014 – website, 18.8.2014)	https://matsne.gov.ge/en/document/download/1561437/7/en/pdf

Title	Types of Data Covered	Selected Rules in Germany on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Ghana

Title	Types of Data Covered	Selected Rules in Ghana on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The primary legislation governing privacy / data protection in Ghana is the Data Protection Act, 2012 (Act 843). Although the law does not contain specific provisions on data transfers, provisions regarding data collection and processing generally provide that a person may collect data from a data subject unless: • the data is contained in a public record • the data subject has deliberately made the data public • the data subject has consented to the collection of the information from another source • the collection of the data from another source is unlikely to prejudice a legitimate interest of the data subject • the collection of the data from another source is necessary for a number of expressly designated purposes (for example the detection or punishment of an offence or breach of law) • compliance would prejudice a lawful purpose for the collection • compliance is not reasonably practicable. A data controller must also ensure that the data subject is aware of, inter alia, the purpose for which the data is required for collection and the recipient of the data.	https://www.dlapiperdataprotection.com/index.html?t=collection-and-processing&c=GH
Data Protection Act (Act No. 843) 2012 (Act of the Parliament of the Republic of Ghana Entitled	Personal	No specific provisions relating to cross border data transfer	https://www.dataguidance.com/sites/default/files/data_protection_act_2012_act_843.pdf

Greece

Title	Types of Data Covered	Selected Rules in Greece on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Guinea

Title	Types of Data Covered	Selected Rules in Guinea on Cross-Border Data Transfers or Data Localization	Sources
LAW L-2016-037-AN on Cybersecurity and Protection of Personal Data	Personal	Not excerpted or summarized due to lack of translation.	https://justiceguinee.gov.gn/laws/loi-l-2016-037-an-relative-a-la-cybersecurite-et-la-protection-des-donnees-a-caractere-personnel/

Honduras

\Title	Types of Data Covered	Selected Rules in Honduras on Cross-Border Data Transfers or Data Localization	Sources
Ley de trasnparencia y accesso a la información pública DECRETO No. 170-2006 (in Spanish)	Personal	Not excerpted or summarized due to lack of translation.	http://www.oas.org/es/sla/ddi/docs/H2%20LeyDeTransparencia.pdf

Hungary

Title	Types of Data Covered	Selected Rules in Hungary on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Iceland

\Title	Types of Data Covered	Selected Rules in Iceland on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	See Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

India

Title	Types of Data Covered	Selected Rules in India on Cross-Border Data Transfers or Data Localization	Sources
DRAFT Digital Personal Data Protection Bill, 2022	Personal	**Digital Personal Data Protection Bill** 17. Transfer of personal data outside India The Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified 18. Exemptions. (1) The provisions of Chapter 2 except sub-section (4) of section 9, Chapter 3 and Section 17 of this Act shall not apply where: (a) the processing of personal data is necessary for enforcing any legal right or claim; (b) the processing of personal data by any court or tribunal or any other body in India is necessary for the performance of any judicial or quasi-judicial function; (c) personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law; (d) personal data of Data Principals not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India. (2) The Central Government may, by notification, exempt from the application of provisions of this Act, the processing of personal data: (a) by any instrumentality of the State in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these; and (b) necessary for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is carried on in accordance with standards specified by the Board. (3) The Central Government may by notification, having regard to the volume and nature of personal data processed, notify certain Data Fiduciaries or class of Data Fiduciaries as Data Fiduciary to whom the provisions of Section 6, sub-sections (2) and (6) of section 9, sections 10, 11 and 12 of this Act shall not apply. (4) The provisions of sub-section (6) of section 9 of this Act shall not apply in respect of processing by the State or any instrumentality of the State.	Digital Personal Data Protection Bill, https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf
Information Technology Act	Personal	At present, the Information Technology Act, 2000 (the Act) and rules notified thereunder largely govern data protection in India. India's IT Ministry adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules), notified under the Act. The Privacy Rules, which took effect in 2011, require corporate entities collecting, processing and storing personal information, including sensitive personal information, to comply with certain procedures. It distinguishes both 'personal information' and 'sensitive personal information.' The data collector must obtain the consent of the provider of the information for any transfer of sensitive personal information to any other corporate entity or person in India, or to any other country that ensures the same level of data protection as provided for under the Privacy Rules. However, consent is not necessary for the transfer if it is required for the performance of a lawful contract between the corporate entity (or any person acting on its behalf) and the provider of information or as otherwise specified in the Act. A corporate entity may not transfer any sensitive personal information to another person or entity that does not maintain the same level of data protection as required by the Act. The contract regulating the data transfer should contain adequate indemnity provisions for a third party breach, should clearly specify the end purposes of the data processing (including who has access to such data) and should specify a mode of transfer that is adequately secured and safe. Further, under the Act, it is an offense for any person who has pursuant to a contract gained access to any material containing personal information to disclose that information without the consent of the person concerned, and with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain.Thus, contracts should also specifically include provisions: • Entitling the data collector to distinguish between 'personal information' and 'sensitive personal information' that it wishes to collect/process, and • Representing that the consent of the person(s) concerned has been obtained for collection and disclosure of personal information or sensitive personal information, and outlining the liability of the third party	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=IN

Title	Types of Data Covered	Selected Rules in India on Cross-Border Data Transfers or Data Localization	Sources
Reserve Bank of India, Amendment to the Master Direction (MD) on Know-Your-Customer, RBI/2021-22/35 (May 10, 2021)	Personal / Financial	Summary: Requires establishment of Video-based Customer Identification Processes (V-CIP) that limit cross-border data transfers, as follows: "(iii) The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses."	Reserve Bank of India, Amendment to the Master Direction (MD) on Know-Your-Customer
Securities and Exchange Board of India, Advisory for on Software as a Service, (Nov. 3, 2020)	Financial	Excerpt: Para 3.: "It is advised to ensure complete protection and seamless control over the critical systems at your organizations by continuous monitoring through direct control and supervision protocol mechanisms while keeping the critical data within the legal boundary of India."	Securities and Exchange Board of India, Advisory for Financial Sector Organizations regarding Software as a Service (SaaS) based solutions
DRAFT National Geospatial Policy (2019)	Geospatial	Excerpt: "Paragraph 8… vii. Maps/Geospatial Data of spatial accuracy/value finer than the threshold value can only be created and/or owned by Indian Entities and must be stored and processed in India. viii. Foreign companies and foreign owned or controlled Indian companies can license from Indian Entities digital Maps/Geospatial Data of spatial accuracy/value finer than the threshold value only for the purpose of serving their customers in India. Access to such Maps/Geospatial Data shall only be made available through APIs that do not allow Maps/Geospatial Data to pass through Licensee Company or its servers. Re-use or resale of such map data by licensees shall be prohibited. ix. Digital Maps/Geospatial Data of spatial accuracy/value up to the threshold value can be uploaded to the cloud but those with accuracy finer than the threshold value shall only be stored and processed on a domestic cloud or on servers physically located within territory of India. x. There shall be no restriction on export of Maps/Geospatial Data of spatial accuracy/value up to the threshold value except for attributes in the negative lists. Department of Revenue, Government of India will make necessary amendments in GSR in this regard	Department of Science and Technology, DRAFT National Geospatial Policy (2019)
Reserve Bank of India, Directive 2017-18/153 (April 6, 2018)	Personal	Excerpt: Para. 2(i): All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required.	Reserve Bank of India, Directive 2017-18/153 (April 6, 2018) Khaitan & Co., Data Localization Laws - India
Consolidated FDI Policy Circular (August 28, 2017)	Subscriber	Summary: Prohibits certain data transfers in connection with foreign direct investment in the broadcasting sector, noting that, "(ix) The Company shall not transfer the subscribers' databases to any person/place outside India unless permitted by relevant law."	DIPP, Consolidated FDI Policy
Guidelines for Government Departments on Contractual Terms		Excerpt: Location of Data	Guidelines for Government Departments on Contractual Terms

Title	Types of Data Covered	Selected Rules in India on Cross-Border Data Transfers or Data Localization	Sources
Related to Cloud Services (March 31, 2017)		The location of the data could be located in one or more discrete sites in foreign countries. Therefore it has to be specifically mentioned in the agreement. The term and conditions of the Empanelment of the Cloud Service Provider has taken care of this requirement by stating that all services including data will be guaranteed to reside in India. Therefore the following clause should be included in the contract: i. The location of the data (text, audio, video, or image files, and software (including machine images), that are provided to the CSP for processing, storage or hosting by the CSP services in connection with the Department's account and any computational results that a Department or any end user derives from the foregoing through their use of the CSP's services) shall be as per the terms and conditions of the Empanelment of the Cloud Service Provider.	Related to Cloud Services (March 31, 2017) https://www.meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf.
Insurance Regulatory & Development Authority of India, Maintenance of Insurance Records Regulations (2015)	Financial	Excerpt: Art. 3(9): The records including those held in electronic mode, pertaining to all the policies issued and all claims made in India shall be held in data centres located and maintained in India only.	Insurance Regulatory & Development Authority of India, Maintenance of Insurance Records Regulations (2015) Khaitan & Co., Data Localization Laws - India

Indonesia

Title	Types of Data Covered	Selected Rules in Indonesia on Cross-Border Data Transfers or Data Localization	Sources
Summary	Various	**This is not current. Needs to be updated.** Article 26 paragraph (2) of Reg. 71 provides that in the implementation of the electronic system which is directed to electronic information and/or electronic document that can be transferred (such as securities (valuable paper) and securities in electronic form), such electronic information and/or electronic document must be unique and explain the possession and ownership. The elucidation of Article 26 paragraph (2) of Reg. 71 further explains the above provision, as follows: • "Electronic information and/or electronic document must be unique" means it is the only one that represents a certain value. • "Electronic information and/or electronic document must explain the possession" means the electronic system has control system or recording system over such electronic information and/or electronic document. • "Electronic information and/or electronic document must explain the ownership" means the electronic system has technology control measures that guarantee that there is only one single authoritative copy and cannot be amended.	
Government Regulation 71 of 2019 regarding the Operation of Electronic Systems and Transactions	Various	Summary: In October 2019, the Government of Indonesia issued Government Regulation 71 on the Operation of Electronic Systems and Transactions (GR71) to supersede and replace GR82. GR71 explicitly clarifies that public sector data must be managed, stored, and processed in Indonesia, but there is no similar restriction on private sector data, which can be managed, stored, and processed anywhere, subject to requirements with respect to financial sector data that may be imposed by the financial sector regulator. Indonesia's reflection of the broad principle in GR71 that "private electronic systems operators" may place their systems and data outside of Indonesia is a positive development. However, so-called "Public Scope Electronic System Providers" are required to store and process data onshore. Additionally, Article 99 of GR 71 states that institutions holding "Strategic Electronic Data" must hold archives and must be connected to a specific data center. "Strategic Electronic Data" encompasses data relating to energy, transportation, financial, healthcare, ICT, food, defense, and other sectors stipulated by the Government	*Government Regulation 71 of 2019 regarding Operation of Electronic Systems and Transactions* BSA, *2021 NTE submission* USTR, *2021 NTE Report*
OJK (Financial Services Authority, Regulations 13/2020 and 38/2020	Financial	Summary: In 2020, OJK issued Regulations 13/2020 and 38/2020, which appear to allow some but not all data to be transferred and stored outside of Indonesia for commercial banks and insurance companies. OJK has confirmed that certain categories of electronic systems, namely front-end systems including those containing individual transaction or customer details, held by banks may be stored outside of Indonesia with OJK's approval.	USTR, *2021 NTE Report* Microsoft, *Financial Services in Indonesia*
Personal Data Protection Bill	Personal	Data Protection Law of Indonesia Division One Transfer of Personal Data within the Jurisdiction of the Republic of Indonesia Article 55 (1) A Personal Data Controller may transfer Personal Data to other Personal Data Controllers within the jurisdiction of the Republic of Indonesia. (2) The Personal Data Controller who transfers Personal Data and who receives the transfer of Personal Data must carry out Personal Data Protection as referred to in this Law. Division Two Transfer of Personal Data to Outside the Jurisdiction of the Republic of Indonesia Article 56 (1) A Personal Data Controller may transfer Personal Data to other Personal Data Controllers and/or Personal Data Processors outside the jurisdiction of the Republic of Indonesia in accordance with the provisions stipulated under this Law.	https://iclg.com/practice-areas/data-protection-laws-and-regulations/indonesia https://www.hukumonline.com/pusatdata/detail/lt561f74edf3260/nprt/481/rancangan-undang-undang-tahun-2019#!

Title	Types of Data Covered	Selected Rules in Indonesia on Cross-Border Data Transfers or Data Localization	Sources
		(2) In carrying out the transfer of Personal Data as referred to in paragraph (1), the Personal Data Controller must ensure that the country of domicile of the Personal Data Controller and/or the Personal Data Processor that receives the transfer of Personal Data has a Personal Data Protection level that is equal to or higher than those that are regulated under this Law (3) In the event that the provisions as referred to in paragraph (2) fail to be fulfilled, the Personal Data Controller must ensure that there is adequate and binding Personal Data Protection. (4) In the event that the provisions as referred to in paragraphs (2) and (3) fail to be fulfilled, the Personal Data Controller must obtain approval of the Personal Data Subject. (5) Further provisions regarding the transfer of Personal Data shall be regulated in a Regulation of the Government.	
Government Regulation 80	Various	Summary: Certain provisions in GR 80 reportedly stipulate that personal data cannot be transferred offshore, unless the receiving nation is deemed by the Ministry of Trade as having equivalent personal data standards and protection as Indonesia.	BSA, *2021 NTE submission*
Government Regulation 17	Add	Add	
Government Regulation 109	Add	Add	
Minister of Communication & Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System ("MOCI Reg. 20/2016")	Personal	Article 21 (1) of MOCI Regulation states that displaying, announcing, transferring, broadcasting, and/or opening personal data access in the electronic system can only be conducted: • by consent (being defined as a written agreement either manually and/or electronically being given by the owner of personal data after obtaining a full explanation regarding the process for acquiring, collecting, processing, analyzing, storing, displaying, announcing, disseminating, storing, dis-playing, announcing, sending, and disseminating including the confidentiality or non-confidentiality of the personal data), except stipulated otherwise by laws and regulations; and • after its accuracy and suitability with the purpose of obtaining and collecting such personal data is verified. Article 22 paragraph (1) of the MOCI Reg. 20/2016 states that transferring personal data that is managed by an electronic system provider at the government and regional government institution including the public or private sector domiciled in the territory of Indonesia to parties outside the territory of Indonesia must: • coordinate with the Minister of Communication and Informatics or the official or institution being authorized for such purpose; and implement the laws and regulations regarding the transboundary exchange of personal data. Article 22 paragraph (2) of the MOCI Reg. 20/2016 further explains that the implementation of the coordination as stipulated in Article 22 paragraph (1) point (a) of MOCI Reg. 20/2016 being: • to report the implementation plan of personal data transfer, at least containing the clear name of the designated country, recipient subject name, implementation date, and reason / purpose of the transfer; • to request for advocacy, if needed; and • to report the activities implementation result.	DLA Piper
Financial Services Authority Regulation No. 38/POJK.03/2016 as partially amended by Financial Services Authority Regulation No. 13/POJK.03/2020 on the Implementation of Risk Management	Financial	Article 21 paragraph (2) of Financial Services Authority Regulation No. 38/POJK.03/2016 as partially amended by Financial Services Authority Regulation No. 13/POJK.03/2020 on the Implementation of Risk Management in the Utilization of Information Technology by the Bank stipulates that the bank's customer data transfer (by way of establishing a data center or a data processing outside Indonesia territory) necessitates prior approval being obtained from the Financial Services Authority ("**FSA**").	DLA Piper

Title	Types of Data Covered	Selected Rules in Indonesia on Cross-Border Data Transfers or Data Localization	Sources
in the Utilization of Information Technology by the Bank			

Ireland

Title	Types of Data Covered	Selected Rules in Ireland on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Title	Types of Data Covered	Selected Rules in Israel on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	he laws that govern the right to privacy in Israel are the Basic Law: Human Dignity and Liberty, 5752 -1992; the Protection of Privacy Law, 5741-1981 and the regulations promulgated thereunder (the 'PPL') and the guidelines of the Israel Privacy Authority. The transfer of personal data abroad is subject to the Privacy Protection Regulations (Transfer of Data to Databases Abroad), 5761-2001, pursuant to which personal data may be transferred abroad only to the extent that: • the laws of the country to which the data is transferred ensure a level of protection, no lesser than the level of protection of data provided for by Israeli Law; or • one of the following conditions is met: o the data subject has consented to the transfer; o the consent of the data subject cannot be obtained and the transfer is vital to the protection of his or her health or physical wellbeing; o the data is transferred to a corporation under the control of the owner of the database from which the data is transferred, provided that such corporation has guaranteed the protection of privacy after the transfer; o the data is transferred to an entity bound by an agreement with the database owner, to comply with the conditions governing the use of the data as applicable under Israeli Laws, mutatis mutandis; o data was made available to the public or was opened for public inspection by legal authority; o transfer of data is vital to public safety or security; o the transfer of data is required by Israeli Law; or o data is transferred to a database in a country: ▪ which is a party to the European Convention for the Protection of Individuals with Regard to Automatic Processing of Sensitive Data; or ▪ which receives data from Member States of the European Community, under the same terms of acceptance[1], or ▪ in relation to which the Registrar of Databases announced, in an announcement published in the Official Gazette (Reshumot), that it has an authority for the protection of privacy, after reaching an arrangement for cooperation with that authority. When transferring personal data abroad, the database owner is required to enter into a data transfer agreement with the data recipient, pursuant to which the recipient undertakes to apply adequate measures to ensure the privacy of the data subjects and guarantees that the data shall not be further transferred to any third party. The foregoing data transfer agreement must also comply with additional restrictions, to the extent that the recipient provides outsourcing services, as set forth in the Outsourcing Guidelines. On January 31, 2011, the European Commission, on the basis of Article 25(6) of directive 95/46/EC, determined that the State of Israel ensures an adequate level of protection with regard to automated processing of personal data. Additionally, the transfer of databases is subject to the IPA Draft Guidelines No. 3/2017, which under certain circumstances, such as database recipient having a conflict of interest, might require opt-in consents of data subjects as a condition to transferring databases.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=IL
PPL	Personal	*The laws that govern the right to privacy in Israel are the Basic Law: Human Dignity and Liberty, 5752 -1992; the Protection of Privacy Law, 5741-1981 and the regulations promulgated thereunder (the 'PPL') and the guidelines of the Israel Privacy Authority (as defined below).*	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Title	Types of Data Covered	Selected Rules in Israel on Cross-Border Data Transfers or Data Localization	Sources
Israel Privacy Authority Guidelines	Personal		

Italy

Title	Types of Data Covered	Selected Rules in Italy on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	See Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Title	Types of Data Covered	Selected Rules in Jamaica on Cross-Border Data Transfers or Data Localization	Sources
THE DATA PROTECTION ACT, 2020 (Act of 2020)	Personal	Excerpt 31.—(1) The eighth standard is that personal data shall not be transferred to a State or territory outside of Jamaica unless that State or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. (2) For the purposes of subsection (1), an adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to— (a) the nature of the personal data; (b) the State or territory of origin of the information contained in the personal data; (c) the State or territory of final destination of that information; (d) the purposes for which and the period during which the personal data are intended to be processed; (e) the law in force in the State or territory in question; (f) the international obligations of that State or territory; (g) any relevant codes of conduct or other rules which are enforceable in that State or territory (whether generally or by arrangement in particular cases); and (h) any security measures taken in respect of the personal data in that State or territory. (3) The eighth standard does not apply to a transfer falling within any of the cases specified in subsection (4), except in such circumstances and to such extent as the Minister may prescribe after consultation with the Commissioner. (4) The cases referred to in subsection (3) are, where— (a) the data subject consents to the transfer; (b) the transfer is necessary— (i) for the performance of a contract between the data subject and the data controller; or (ii) for the taking of steps at the request of the data subject with a view to the data subject entering into a contract with the data controller; (c) the transfer is necessary for the conclusion or performance of a contract, between the data controller and a person other than the data subject, which— (i) is entered into at the request of the data subject; (ii) is in the interests of the data subject; (d) the transfer is necessary for reasons of substantial public interest; (e) the transfer— (i) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings); (ii) is necessary for the purpose of obtaining legal advice; or (iii) is otherwise necessary for the purpose of establishing, exercising, or defending, legal rights; (f) the transfer is necessary in order to protect the vital interests of the data subject; (g) the transfer is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the personal data are or may be disclosed after the transfer;	https://japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202020.pdf

Title	Types of Data Covered	Selected Rules in Jamaica on Cross-Border Data Transfers or Data Localization	Sources
		(h) the transfer is made on terms (which may include contractual terms) that are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects; (i) the transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects (j) the transfer is necessary for the purposes of national security or the prevention, detection or investigation of crime. (5) The Minister may prescribe, by order published in the Gazette— (a) circumstances in which a transfer is to be taken for the purposes of subsection (4)(d) to be necessary for reasons of substantial public interest; (b) circumstances in which a transfer which is not required by or under an enactment is not to be taken for the purposes of subsection (4)(d) to be necessary for reasons of substantial public interest; and (c) the States and territories which shall be taken to have an adequate level of protection within the meaning of subsection (2). (6) For the purposes of subsection (5)(c)— (a) a State or territory having an adequate level of protection as described in that subsection shall be included in the order only if such inclusion is necessary for the fulfilment of Jamaica's international obligations; and (b) the order may provide for such conditions and restrictions as may be applicable under the international obligation concerned. (7) Where any question arises as to whether a transfer may be made to a State or territory, other than a State or territory included in an order made under subsection (5)(c), the matter shall be determined by the Commissioner, who shall issue a notice stating— (a) the relevant public authority with responsibility for the protection of personal data in the State or territory concerned; (b) the Commissioner's determination as to the adequacy of the level of protection (within the meaning of subsection (2)) in the State or territory concerned; and (c) where the Commissioner determines that the level of protection is not adequate, the extent to which the Commissioner considers that the level of protection is not adequate.	

Japan

Title	Types of Data Covered	Selected Rules in Japan on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The Act on the Protection of Personal Information ("APPI") regulates privacy protection issues in Japan and the Personal Information Protection Commission ("PPC"), a central agency acts as a supervisory governmental organization on issues of privacy protection. The APPI was originally enacted in 2003 but was amended and the amendments came into force on 30 May 2017. On 5 June 2020, the Japanese Diet approved a bill to further amend the APPI ("Amended APPI"). The Amended APPI will come into force on April 1, 2022. Currently, Personal Data (meaning Personal Information stored in a database) may not be disclosed to a third party without the prior consent of the individual, unless the business operator handling the Personal Information adopts the opt-out method, provides an advance notice of joint use to data subjects, in the case of merger/business transfer or entrusting the handling of Personal Information to third party service providers. Even disclosing the Personal Information within group companies is considered disclosing the Personal Information to a third party and consent must be obtained, unless it meets the requirements of joint use. The APPI also has permitted the "opt out" method, whereby a business operator can as a default disclose Personal Information to third parties, unless individuals opt out of allowing the business operator to do so. The Amended APPI stipulates that Personal Information that has been transferred from others through the opt out measure or that has obtained by illegal manners, and Sensitive Personal Information cannot be transferred through the opt out measure. The APPI requires a business operator to preemptively disclose to the PPC, and the public or to the data subject of certain items listed below concerning opt out. • the name, address and representative person of the business operator; • the fact that the purpose of use includes the provision of such information to third parties; • the nature of the Personal Information being provided to third parties; • the method by which Personal Information has been obtained; • the method by which Personal Information will be provided to third parties; • the matter that provision of such information to third parties will be stopped upon the request by the data subject; • the method for an individual to submit an opt out request to the business operator; • the method to update Personal Information which has been provided to their parties; and • the schedule date of provision of Personal Information. The APPI does not provide any examples of how best to obtain consent from individuals before sharing Personal Information. Generally, written consent should be obtained whenever possible. When obtaining consents, it would be prudent to clearly disclose to the data subject the identity of the third party to whom the Personal Information will be disclosed, the contents of the Personal Information and how the third party will use the provided Personal Information. The guidelines issued by the PPC provide the following examples as appropriate methods of obtaining the consent for disclosing Personal Information from the data subject: • receipt of confirmation of the oral or written consent (including a record created by electronically or magnetically methods or any other method not recognizable to human senses) from data subject • receipt of a consent email from data subjects • the data subject's check of the confirmation box concerning the consent • the data subject's click of a button on the website concerning the consent, and • the data subject's audio input, or touch of a touch panel concerning the consents If Personal Information is to be used jointly, the business operator could, prior to the joint use, notify the data subjects of or publish the following: • the fact that the Personal Information will be used jointly • the item of the Personal Information to be disclosed • the scope of the joint users • the purpose for which the Personal Information will be used by them, and	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=JP

Title	Types of Data Covered	Selected Rules in Japan on Cross-Border Data Transfers or Data Localization	Sources
		• the name, address and representative person of the business operator responsible for the management of the Personal Information. Transfer of Personally Referable Information The Amended APPI stipulates that prior consent from data subjects is necessary if Personally Referable Information is transferred to a third party and the receiving party can identify a specific individual by way of referencing such Personally Referable Information with any information that the receiving party already has in its possession. In general, such consents are to be obtained by the receiving party and therefore, the transferor needs to, in advance to transferring Personally Referable Information to a third party, confirm if the receiving party has already obtained consents. That being said, it is possible that the transferor collects data subjects' consents on behalf of the receiving party. Cross-border Transfer Under the APPI, in addition to the general requirements for third party transfer, prior consent of data subjects specifying the receiving country is required for transfers to third parties in foreign countries unless the foreign country is white-listed under the enforcement rules of the APPI or the third party receiving Personal Information has established similarly adequate standards for privacy protection as specified in the enforcement rules of the APPI. Currently, UK and EU countries are specified as white-listed countries based on the adequacy decision on January 23, 2019. According to the enforcement rules of the APPI, "similarly adequate standards" means that the practices of the business operator handling the Personal Information are at least equal with the requirements for protection of Personal Information under the APPI or that the business operator has obtained recognition based on international frameworks concerning the handling of Personal Information. According to the guidelines for offshore transfer, one of the examples of an acceptable international framework is the APEC CBPR system. With regard to data subject's consents to transfer their Personal Information to foreign countries, the Amended APPI stipulates that the business operator shall provide the following information to the data subject when obtaining consents therefrom: (i) name of the country where the receiving party resides, (ii) data protection law system in the country and (iii) the data protection measures that the receiving party implements. In addition, the business operator needs to take necessary measures to ensure that the receiving party of such Personal Information continuously takes proper measures to process the Personal Information in a manners equivalent to the requirements of the APPI.	
Amended Act on the Protection of Personal Information (The Amendment Bill of the Act on the Protection of Personal Information, etc., submitted to the ordinary session (201st Session) of the Diet on 10th March 2020, was approved by the Diet on 5th June 2020 and promulgated on 12th June 2020.)	Personal	Excerpt **(Restriction on Third Party Provision)** **Article 23** (1) A personal information handling business operator shall, except inthose cases set forth in the following, not provide personal data to a third party without obtaining in advance a principal's consent. (i) cases based on laws and regulations (ii) cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent (iii) cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent (iv) cases in which there is a need to cooperate in regard to a central government organization or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said affairs (2) A personal information handling business operator, in regard to personal data provided to a third party, may, in cases where it is set to cease in response to a principal's request a third-party provision of personal data that can identify the principal and when pursuant to rules of the Personal Information Protection Commission it has in advance informed a principal of those matters set forth in the following or put them into a state where a principal can easily know, and notified them to the Personal Information Protection Commission, provide the said personal data to a third party notwithstanding the provisions of the preceding paragraph. This, however, shall not apply in cases where personal data provided to a third party is a special care-required personal information, or, has been acquired in violation of the provisions of Article 17 or has been provided by another personal information handling business operator pursuant to the provisions in the main clause of this paragraph (including their wholly or partially duplicated or processed ones). (i) The name or appellation and address and, for a corporate body, the name of its representative (for a non-corporate body having appointed a representative or administrator, the said representative or administrator; hereinafter the same in this Article, Article 26, paragraph (1), item (i), and Article 27, paragraph (1), item (i)) of a personal information handling business operator that provides to a third party. (ii) to set a third-party provision as a utilization purpose (iii) the categories of personal data provided to a third party	Amended Act on the Protection of Personal Information(June 2020) (Tentative Translation) - Personal Information Protection Commission, Japan- (ppc.go.jp)

Title	Types of Data Covered	Selected Rules in Japan on Cross-Border Data Transfers or Data Localization	Sources
		(iv) a method of acquiring personal data provided to a third party (v) a method of a third-party provision (vi) to cease, in response to a principal's request, a third-party provision of personal data that can identify the principal (vii) a method of receiving a principal's request (viii) other matters prescribed by rules of the Personal Information Protection Commission as those necessary to protect an individual's rights and interests (3) A personal information handling business operator shall, in case of those matters set forth in item (i) of the preceding paragraph are altered or when the personal data provision is stopped pursuant to the provisions of the preceding paragraph, without delay, and when intending to alter those matters set forth in item (iii) to item (v), item (vii) or item (viii) of the preceding paragraph, in advance inform a principal to that effect or put them into a state where a principal can easily know and notify them to the Personal Information Protection Commission pursuant to rules of the Personal Information Protection Commission. (4) The Personal Information Protection Commission shall, when notified pursuant to paragraph (2), disclose to the public a matter relating to the notification pursuant to rules of the Personal Information Protection Commission. The same shall apply when notified pursuant to the preceding paragraph. (5) In those cases set forth in the following, a person receiving the provision of the said personal data shall not fall under a third party in regard to applying the provisions of each preceding paragraph. (i) cases in which personal data is provided accompanied by a personal information handling business operator entrusting a whole or part of the handling of the personal data within the necessary scope to achieve a utilization purpose (ii)cases in which personal data is provided accompanied with business succession caused by a merger or other reason (iii) cases in which personal data to be jointly utilized by a specified person is provided to the specified person, and when a principal has in advance been informed or a state has been in place where a principal can easily know to that effect as well as of the categories of the jointly utilized personal data, the scope of a jointly utilizing person, the utilization purpose for the utilizing person and the name or appellation and address, and, for a corporate body, the name of its representative of a person responsible for controlling the said personal data (6) A personal information handling business operator shall, in case of altering the name, appellation or address, or, for a corporate body, the name of its representative of a person responsible for controlling personal data prescribed in item (iii) of the preceding paragraph, without delay, and in case of altering a utilization purpose for a utilizing person or the person responsible prescribed in item (iii) of the preceding paragraph, in advance inform a principal of the contents to be altered or put them into a state where a principal can easily know. **(Restriction on Provision to a Third Party in a Foreign Country)** **Article 24** (1) A personal information handling business operator, except in those cases set forth in each item of the preceding Article, paragraph (1), shall, in case of providing personal data to a third party (excluding a person establishing a system conforming to standards prescribed by rules of the Personal Information Protection Commission as necessary for continuously taking action equivalent to the one that a personal information handling business operator shall take concerning the handling of personal data pursuant to the provisions of this Section (referred to as "equivalent action" in paragraph (3)); hereinafter the same in this paragraph, the succeeding paragraph and Article 26-2, paragraph (1), item(ii)) in a foreign country (meaning a country or region located outside the territory of Japan; hereinafter the same) (excluding those prescribed by rules of the Personal Information Protection Commission as a foreign country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an ndividual's rights and interests; hereinafter the same in this Article and the succeeding paragraph, and, Article26-2, paragraph (1), item (ii)), in advance obtain a principal's consent to the effect that he or she approves the provision to a third party in a foreign country. In this case, the provisions of the preceding Article shall not apply. (2) A personal information handling business operator shall, in case of intending to obtain a principal's consent pursuant to the provisions of the preceding paragraph, in advance provide the principal with information on the personal information protection system of the foreign country, on the action the third party takes for the protection of personal information, and other information that is to serve as a reference to the principal, pursuant to rules of the Personal Information Protection Commission. (3) A personal information handling business operator shall, when having provided personal data to a third party (limited to person establishing a system prescribed in paragraph (1)) in a foreign country, pursuant to rules of the Personal Information Protection Commission, take necessary action to ensure continuous implementation of the equivalent action by the third party, and, in response to a principal's request, provide information on the necessary action, to the principal **(Restriction on Third Party Provision of Personally Referable Information)** **Article 26-2**	

Title	Types of Data Covered	Selected Rules in Japan on Cross-Border Data Transfers or Data Localization	Sources
		(1) A personally referable information handling business operator (meaning a person providing a personally referable information database etc. (Meaning a collective body of information comprising personally referable information (Meaning information relating to a living individual which does not fall under personal information, pseudonymously processed information or anonymously processed information; the same applies hereinafter) which has been systematically organized so as to be able to search using a computer for specific personally referable information or similar others prescribed by cabinet order as systematically organized so as to be able to search easily for specific personally referable information; the same applies hereinafter) for use in business, however, excluding a person set forth in each item of Article 2, paragraph (5); the same applies hereinafter) shall, if it is assumed that a third party will acquire personally referable information (limited to those constituting personally referable information database etc.; the same applies hereinafter) as personal data, except in those cases set forth in each item of Article 23, paragraph (1), not provide the personally referable information to a third party without confirming those matters set forth in the following pursuant to rules of the Personal Information Protection Commission.\ (i)The principal's consent to the effect that he or she approves that the third party acquires personally referable information as personal data that can identify the principal receives the provision of personally referable information from handling business operator, has been obtained. (ii)For a provision to a third party in a foreign country, in case of intending to obtain the principal's consent referred to in the preceding item, pursuant to rules of the Personal Information Protection Commission, information on the personal information protection system of the foreign country, on the action the third party takes for the protection of personal information, and other information that is to serve as a reference to the principal, have been provided in advance to the principal. (2) The provisions of Article 24, paragraph (3) shall apply mutatis mutandis to the case that a personally referable information handling business operator provides personally referable information pursuant to the provisions of the preceding paragraph. In this case, the term "take necessary action to ensure continuous implementation of the equivalent action by the third party, and, in response to a principal's request, provide information on the necessary action, to the principal." in Article 24, paragraph (3) is deemed to be replaced with "take necessary action to ensure continuous implementation of the equivalent action by the third party." (3) The provisions of preceding Article, paragraph (2) through paragraph (4) shall apply mutatis mutandis to the case that a personally referable information handling business operator confirms pursuant to the provisions of paragraph (1). In this case, the term "received the provision of" in the preceding Article, paragraph (3) is deemed to be replaced with "provided." **Chapter VI Miscellaneous Provisions** **(Scope of Application)** **Article 75** This Act shall also apply in those cases where a personal information handling business operator etc., in relation to supplying a good or service to a person in Japan, handles the personal information that has a person in Japan as the principal, personally referable information that is to be acquired as the said personal information, pseudonymously processed information or anonymously processed information produced by using the said personal information, in a foreign country. **(Exclusion from Application)** **Article 76** (1) To a person set forth in each following item who is a personal information handling business operator shall the provisions of Chapter IV not apply when a whole or part of the purpose of handling personal information etc. is a purpose prescribed in each said item respectively. (i)a broadcasting institution, newspaper publisher, communication agency and other press organization (including an individual engaged in the press as his or her business): a purpose of being provided for use in the press (ii) a person who practices writing as a profession: a purpose of being provided for use in writing (iii) a university and other organization or group aimed at academic studies, or a person belonging thereto: a purpose of being provided for use in academic studies (iv) a religious body: a purpose of being provided for use in a religious activity (including those activities accessory thereto) (v) a political body: a purpose of being provided for use in a political activity (including those activities accessory thereto) (2) The "press" prescribed in item (1) of the preceding paragraph means informing a large number of unspecified people of an objective fact as such (including stating an opinion or view based thereon).	

Title	Types of Data Covered	Selected Rules in Japan on Cross-Border Data Transfers or Data Localization	Sources
		(3) A personal information handling business operator etc. set forth in each item of paragraph (1) shall strive to take itself necessary and appropriate action for the security control of personal data, pseudonymously processed information or anonymously processed information and necessary action to ensure the proper handling of personal information etc. (excluding personally referable information; hereinafter the same applies in this paragraph) such as dealing with a complaint about the handling of personal information etc., as well as announce to the public the contents of such action taken. **(Information Provision to the Foreign Enforcement Authorities)** **Article 78** (1) The Commission may provide the foreign authorities enforcing those foreign laws and regulations equivalent to this Act (hereinafter referred to as the "foreign enforcement authorities" in this Article) with information recognized as contributory to fulfilling their duties (limited to those equivalent to the Commission's duties prescribed in this Act; the same shall apply in the succeeding paragraph). (2) Concerning the provision of information pursuant to the preceding paragraph, appropriate action shall be taken so that the information is neither used for purposes other than for the foreign enforcement authorities fulfilling their duties nor used for a foreign criminal case investigation (limited to the one conducted after the criminal facts subject to the investigation have been specified) or adjudication (hereinafter collectively referred to as an "investigation etc.") without consent pursuant to the succeeding paragraph. (3) The Commission may, when having received a request from the foreign enforcement authorities, consent that the information it provided pursuant to paragraph (1) be used for a foreign criminal case investigation etc. in connection with the request except for those cases falling under any of each following item. (i)when a crime subject to the criminal case investigation etc. in connection with the said request is a political crime, or when the said request is recognized to have been made for the purpose of conducting the investigation etc. into a political crime (ii) when an act relating to the crime subject to a criminal case investigation etc. in connection with the said request, if it were committed in Japan, shall not constitute a criminal offense according to the laws and regulations in Japan (iii) when there is no assurance that the requesting country will accept the same kind of request from Japan (4) The Commission shall, in case of consenting under the preceding paragraph, obtain a Minister of Justice's confirmation of the case not falling under item (i) and item (ii) of the preceding paragraph, and a Minister of Foreign Affairs' confirmation of the case not falling under item (iii) of the preceding paragraph respectively. **(Sincere Implementation of International Agreements etc.)** **Article 78-2** In the enforcement of this Act, care must be taken not to prevent the sincere implementation of treaties and other international agreements which Japan has concluded, and established international law must be complied with.	
Personal Information Protection Commission of Japan, Rules re the Protection of Personal Information	Personal	Article 11-3 of Commission Rules (1) The method of providing information pursuant to the provision of Article 24, paragraph (2) of the Act or Article 26-2, paragraph (1), item (ii) of the Act shall be the method of providing electromagnetic records, the method of delivering documents, or any other appropriate method. (2) The provision of information pursuant to the provision of Article 24, paragraph (2) of the Act or Article 26-2, paragraph (1), item (ii) of the Act shall be made with regard to the following matters. (i) name of the said foreign country (ii) information on the system relating to the protection of personal information in the foreign country, obtained by an appropriate and reasonable method. (iii) information on the action to be taken by the third party to protect personal information. (3) Notwithstanding the provisions of the preceding paragraph, if the matter set forth in item (i) of the preceding paragraph cannot be specified at the time of obtaining the consent of the principal pursuant to the provisions of Article 24, paragraph (1) of the Act, the business operator handling personal information shall provide information on the following matters in lieu of the matters specified in the same item and item (ii) of the same paragraph. (i) The fact that the matter set forth in item (i) of the preceding paragraph cannot be specified and the reason therefor. (ii) If there is information that can be used as a reference for the principal in lieu of the matter set forth in item (i) of the preceding paragraph, such information.	

Title	Types of Data Covered	Selected Rules in Japan on Cross-Border Data Transfers or Data Localization	Sources
		(4) Notwithstanding the provisions of paragraph (2), if, at the time of obtaining consent from a principal pursuant to the provisions of Article 24, paragraph (1) of the Act, the business operator handling personal information is unable to provide information on the matter set forth in item (iii) of paragraph (2), the business operator handling personal information shall provide information to that effect and the reason therefor in lieu of the matter set forth in the same item. Article 11-4 of Commission Rules (1) The action necessary to ensure the continuous implementation of the equivalent action by a third party in a foreign country pursuant to the provisions of Article 24, paragraph (3) of the Act (including the case in which it is applied mutatis mutandis upon replacement of the term in Article 26-2, paragraph (2) of the Act) shall be as follows. (i) periodic confirmation, in a reasonable and appropriate manner, of the status of implementation of the action taken by the relevant third party, as well as the existence or non-existence of the relevant foreign country's system and its contents that may affect the implementation of the action. (ii) If an obstacle arises in the implementation of the action by the third party, take necessary and appropriate action, and if it becomes difficult to ensure the continuous implementation of the action, suspend the provision of personal data (or personally referable information in the case of applying mutatis mutandis upon replacement of the term in Article 26 -2, paragraph (2)) to the third party. (2) The method of providing information pursuant to the provisions of Article 24, paragraph (3) of the Act shall be by providing an electronic record, by delivering a written document, or by any other appropriate method. (3) Upon receiving a request pursuant to the provisions of Article 24, paragraph (3) of the Act, a business operator handling personal information shall provide the principal with information on the following matters without delay. However, if the provision of the information is likely to cause significant hindrance to the proper performance of the duties of the business operator handling the personal information, the provision of all or part of the information may be withheld. (i) the method of establishment of the system prescribed in Article 24, paragraph (1) of the Act by the said third party (ii) outline of the action to be implemented by the said third party (iii) frequency and method of confirmation pursuant to the provision of paragraph (1), item (i) (iv) name of the said foreign country. (v) existence or non-existence of a system in the foreign country that may affect the implementation of the action by the third party, and a summary thereof (vi) existence or nonexistence of any impediment to the implementation of the actions by the said third party, and a summary thereof (vii) summary of the action to be taken by the business operator handling the personal information pursuant to the provisions of paragraph 1, item 2 in relation to the impediment set forth in the preceding item. (4) When a business operator handling personal information decides not to provide all or part of the information requested pursuant to the provisions of Article 24, paragraph (3) of the Act, the business operator handling personal information shall notify the principal to that effect without delay. (5) When a business operator handling personal information notifies that it will not provide all or part of the information requested by the principal pursuant to the preceding paragraph, the business operator shall endeavor to explain the reasons to the principal.	
PPC Guidelines for the Act on the Protection of Personal Information (“Provision to a Third Party in a Foreign Country”)	Personal	Guidelines for the Act on the Protection of Personal Information (“Provision to a Third Party in a Foreign Country”) 5. Provision of Information at the Time of Obtaining Consent When personal information handling business operator intends to obtain a consent of a principal to allow the provision of personal data to a third party located in a foreign country pursuant to Article 24, paragraph 1 of the Act, it must provide the principal with the required information pursuant to Article 11-3, paragraphs 2 through 4 of the Commission Rules (Article 24, Paragraph 2 of the Act) (*). In the case of a cross-border transfer of personal data, the personal information handling business operator which is the provider of personal information must evaluate the risks involved in transferring personal data to a foreign country where the third party is located and examine the necessity of transferring the personal data. It is important to provide easy-to-understand information to the principal concerned. The information must be provided to the principal in an appropriate manner that ensures that the principal can recognize the required information pursuant to the stipulation of Article 11-3, paragraphs 2 through 4. It is important that the information to be provided is easy for the principal to understand. [Examples that fall as "appropriate method”] Example 1) sending the necessary information to the principal by e-mail Example 2) direct delivery of a document containing the necessary information to the principal Example 3) verbally explaining necessary information to the principal Example 4) posting the required information on a website and making it available to the principal.	

Title	Types of Data Covered	Selected Rules in Japan on Cross-Border Data Transfers or Data Localization	Sources
		5-2 Information to be Provided (related to Article 11-3, paragraph 2 of Commission Rules) When obtaining consent of a principal to allow the provision of personal data to a third party in a foreign country, the following (1) to (3) must be provided to the principal. (1) “name of the “said foreign country” (related to Article 11-3, paragraph 2, (i) of Commission Rules) This refers to the name (*2) of the foreign country (*1) in which the third party recipient is located. Although an official name is not necessarily required, it must be a name that is considered to enable the principal to reasonably recognize the location to which his/her personal data will be transferred. For details on how to handle cases in which the foreign country where the third party to be provided is located cannot be specified upon the time of obtaining the consent of the principal to allow the provision of personal data to a third party located in a foreign country, refer to 5-3-1 (Cases in which the foreign country where the third party to be provided is located cannot be specified). (*1) "Foreign country" means a country or region outside of Japan and excludes a foreign country establishing a personal information protection system recognized to have equivalent standards to that in Japan as stipulated in Commission Rules (Article 24, paragraph 1 of the Act). (*2) It is sufficient to provide the name of the foreign country where the third party is located, and it is not required to additionally provide the name of the state where the third party is located. However, in light of the purpose of the system to increase the predictability of the principal with respect to the risks associated with cross-border transfers of personal data, if, for example, state law is a major discipline and the provision of information on state law will contribute to increasing the individual's predictability, it is desirable to indicate the state where the foreign third party is located and provide information about the system at the state level. (2) "information on the system relating to the protection of personal information in the said foreign country, obtained by an appropriate and reasonable method” (related to Article 11-3, paragraph 2, Item (ii) of Commission Rules) 1) "appropriate and reasonable method” The "information relating to the protection of personal information in the said foreign country" shall be confirmed by an appropriate and reasonable method with general attention. [Examples of appropriate and reasonable methods] Example 1) inquiry to a third party in a foreign country to which the personal information is provided Example 2) confirmation of information published by an administrative organ, etc. in Japan or a foreign country 2) "information on the system relating to the protection of personal information in the said foreign country” In light of the purpose of the system to increase the predictability of the principal regarding the risks associated with cross-border transfers of personal data, "information relating to the system for the protection of personal information in the said foreign country" must be information that enables the principal to reasonably recognize the essential differences between the system for the protection of personal information in which the third party recipient is located and the law in Japan (Act on the Protection of Personal Information). Specifically, the following points (a) through (d) must be taken into consideration. In addition, the "system for the protection of personal information in the said foreign country" here is limited to the system in the said foreign country that applies to the third party recipient in the foreign country, and does not include systems that do not apply to the third party. (a) Existence or non-existence of a system for the protection of personal information in the said foreign country If there is no system for the protection of personal information applicable to the third party recipient in the said foreign country, this in itself indicates the existence of a risk associated with the cross-border transfer of personal data. Therefore, information must be provided to the principal to the effect that a system for the protection of personal information does not exist. (*1). (b) The existence of information that can serve as an indicator of the foreign country's system for the protection of personal information. In the case in which information exists that could serve as an objective indicator of the level of protection of personal information, etc., with respect to the system for the protection of personal information in the said foreign country in which the third party recipient is located, the provision of such informationwould be considered to guarantee, to a certain extent, the principal's predictability of the risks associated with the cross-border transfer of personal data. Therefore, in this case, it is sufficient to provide information that can serve as an indicator, and the provision of information related to (c) below is not required.	

Title	Types of Data Covered	Selected Rules in Japan on Cross-Border Data Transfers or Data Localization	Sources
		It is also desirable to provide the principal with information on what the potential indicator information means in relation to the risks associated with the cross-border transfer of personal data. [Examples of information that may serve as an indicator of the foreign country's personal information protection system] Example 1) The foreign country where the said third party is located is a country that has obtained adequacy determination based on Article 45 of the GDPR. Example 2) The foreign country in which the said third party is located is a participating country of the APEC CBPR system. (c) Non-existence of obligations of the business operator or rights of the principal corresponding to the 8 OECD Principles In the event that the obligations of the business operator or the rights of the principal corresponding to 8 Principles OECD Privacy Guidelines (*2) do not exist in the foreign country where the third party recipient is located, the absence of the obligations of the business operator or the rights of the principal shall be deemed to be an essential difference with the laws of Japan (Act on the Protection of Personal Information). Therefore, such information must be provided to the principal. If the system for the protection of personal information in the foreign country in which the third party recipient is located includes all the obligations of the business operator and the rights of the principal corresponding to the 8 Principles of OECD Privacy Guidelines, it is sufficient to provide information to that effect to the principal. [Examples absence of obligations of the business or rights of the principal corresponding to 8 Principles of the OECD Privacy Guidelines] Example 1) non-existence of restriction that personal information must, in principle, be used within the scope of utilization purpose specified in advance Example 2) non-existence of the right of the principal to request disclosure of personal information held by business operators (d) Existence of other systems that may have a significant impact on the rights and interests of the principal If, in comparison with the system in Japan, a system exists in a foreign country in which the third party recipient is located that may have a significant impact on the rights and interests of the principal whose personal data is transferred to that foreign country, the principal must be informed of the existence of the said system. [Examples of systems that may have a significant impact on the rights and interests of the principal] Example 1) a system that allows the government to collect a wide range of information on personal information held by businesses operators by imposing on businesses operators an obligation to cooperate extensively with government information collection activities. Example 2) a system pertaining to the obligation to preserve personal information within the country which may not enable business operators to respond to a request for deletion, etc. from a principal. (*1) If a system for the protection of personal information exists in a foreign country in which the third party recipient is located, it is not required to provide the individual names of the laws and regulations pertaining to the system to a principal, however, it is desirable to be able to provide such information upon request. (*2) The OECD Privacy Guidelines are based on the following basic principles: 1) Collection Limitation Principle, 2) Data Quality Principle, 3) Purpose Specification Principle, 4) Use Limitation Principle 5) Security Safeguards Principle, 6) Openness Principle, 7) Individual Participation Principle, 8) Accountability Principle. (3) “Information on the action to be taken by the third party to protect personal information” (relating to Article 11-3 Article, paragraph 2, item (iii) of Commission Rules) In light of the purpose of the system to increase the predictability of the principal with respect to risks associated with cross-border transfers of personal data, "information on the action taken by the third party to protect personal information" shall include information that enables the principal to reasonably understand the essential differences between the action for the protection of personal information taken by a third party in the said foreign country and the action required under the Japanese law (Act on the Protection of Personal Information) of a personal information handling business operator. Specifically, if the third party in the foreign country has not taken action to comply with the 8 principles of OECD Privacy Guidelines (including action to respond to a request based on the rights of the principal), the principal shall be informed of the details of the action not taken. If the third party recipient in the said foreign country has taken all the actions required by the 8 principles of OECD Privacy Guidelines, it is sufficient to provide the principal with information to that effect.	

Title	Types of Data Covered	Selected Rules in Japan on Cross-Border Data Transfers or Data Localization	Sources
		Please refer to 5-3-2 (Cases in which information on action taken by a third party to protect personal information cannot be provided) for the handling regarding the case in which information of the action to be taken by the foreign third party to protect personal information cannot be provided when obtaining a consent from a principal to allow the provision of personal data to a foreign third party. [Examples of provision of information regarding the action taken by the third party recipient to protect personal information (when the third party recipient has not notified or publicly released utilization purpose)] Example) Information to be provided to the effect that "the recipient generally takes action equivalent as those required of personal information handling business operators in Japan for the handling of personal data, however, does not notify or publicly disclose utilization purpose of the personal information obtained". 5-3 Handling in cases in which personal information handling business operator is unable to specify the recipient when obtaining consent (related to Article 11-3, paragraph 4 of Commission Rules) 5-3-1 Cases in which the foreign country of the third party recipient cannot be specified (related to Article 11-3, Paragraph 3 of Commission Rules) If, at the time of obtaining a consent of a principal to allow the provision of personal data to a third party located in a foreign country pursuant to the provisions of Article 24, paragraph 1 of the Act, the foreign country of the third-party recipient cannot be specified, information in the below (1) and (2) may be substituted for the name of the foreign country and information on its system for protecting personal information. If the foreign country of the third party recipient can be identified after the fact, it is desirable to provide the information at the request of the principal. [Examples in which the foreign country of the third party recipient cannot be identified] Example 1) When a pharmaceutical company in Japan is conducting research and development of a drug, etc., and at the time of a doctor etc. responsible for the drug trial explaining to research participants and obtaining their consent, it is not clear to which country's review authority, etc. the application for approval will ultimately be submitted and the foreign country in which the research participants' personal data will be transferred cannot be specified. Example 2) When an insurance company in Japan provides reinsurance to a foreign reinsurance company for the purpose of diversifying underwriting risks, etc., and at the time the insurance company in Japan underwrite and obtain consent from the customer, it is not clear to which reinsurance company reinsurance will ultimately be provided, and the foreign country in which the customer's personal data cannot be specified. (1) The fact and the reason for not being able to specify (related to Article 11-3, paragraph 3, item (i) of Commission Rules) Even in the case in which the foreign country of the third party recipient cannot be specified, the personal information handling business operator shall take into consideration the purpose of improving the principal's predictability of the risks associated with the cross-border transfer and must provide the fact and the reason the foreign country of the third party recipient cannot be specified. In addition, when providing information, it is desirable to explain in detail under what circumstances personal data will be provided to a third party in a foreign country. (2) Information that can be used as a reference for the principal in place of the name of the foreign country in which the third party recipient is located (related to Article 11-3, paragraph 3, item (ii) of Commission Rules) Even if the foreign country in which the third party recipient is located cannot be specified, if it is possible to provide information that can be used as a reference for the principal in place of the name of the foreign country in which the third party recipient is located, such information must also be provided to the principal. The applicability of "information to be used as reference in place of the name of the foreign country in which the third party recipient is located" shall be determined on a case-by-case, however, for example, if the scope of the foreign country of the recipient is specifically determined, information regarding the said scope is considered to be "information that can be used as a reference for the principal in place of the name of the foreign country in which the third party recipient is located". [Examples of information that falls as information that can be used as reference to the principal in place of the name of the foreign country in which the third party recipient is located] Example) In a case in which the name of the candidate foreign country has been specifically determined at the time of obtaining a consent from a principal, the name of the said foreign country. 5-3-2 Cases in which information on the action taken by the third party recipient to protect personal information cannot be provided (related to Article 11-3, paragraph 4 of Commission Rules) If, at the time of obtaining a consent from a principal to allow the provision of personal data to a third party located in a foreign country pursuant to Article 24, paragraph 1 of the Act, the personal information handling business operator is unable to provide information regarding the action for the protection of personal information taken by the third party recipient located in a foreign country, the personal information handling business operator shall provide this fact and the reason for not being able to provide such information. In providing the information, it is desirable to explain in detail under what situations personal data will be provided to a third party located in a foreign country. In addition, when it becomes possible to provide information on the action taken by the said third party to protect personal information after the fact, it is desirable to provide such information upon the request of the principal.	

Title	Types of Data Covered	Selected Rules in Japan on Cross-Border Data Transfers or Data Localization	Sources
		[Examples in which the provision of information on the action taken by the third-party recipient to protect personal information is not possible] Example 1) When a pharmaceutical company in Japan is conducting research and development of a drug, etc., and at the time of a doctor etc. responsible for the drug trial explaining to research participants and obtaining their consent, it is not clear to which country's review authority, etc. the application for approval will ultimately be submitted and the foreign country in which the research participants' personal data will be transferred cannot be specified. Example 2) When an insurance company in Japan provides reinsurance to a foreign reinsurance company for the purpose of diversifying underwriting risks, etc., and at the time the insurance company in Japan underwrite and obtain consent from the customer, it is not clear to which reinsurance company reinsurance will ultimately be provided, and the third party recipient of the customer's personal data cannot be specified. 6. Action, etc., to be taken when personal data is provided to a party that has established a system necessary to continuously take measures equivalent to those that should be taken by a personal information handling business operator. In a case in which a personal information handling business operator provides personal data to a third party that has established a system that conforms to the standards set forth in Article 11-2 of the Commission Rules (hereinafter referred to as the "system that conforms to the standards"), the personal information handling business operator must take necessary action to ensure continuous implementation of the equivalent action by the third party (equivalent to the action taken by personal information handling business operator on the handing of personal data pursuant Article 4, paragraph 1 of the Act. The same shall apply hereinafter), and, in response to a principal's request, provide information on the necessary action, to the principal. (Article 24-3 of the Act) (*) Article 24, paragraph 3 of the Act clarifies that when personal data is provided to a third party in a foreign country on the basis that the recipient has established a system that conforms to the standards, the personal information handling business operator is responsible for continuously ensuring the proper handling of the said personal data by the said third party afterwards. For this reason, personal information handling business operator is required to take action, etc. based on Article 24, paragraph 3 of the Act, as long as the third party continues to handle the said personal data. However, in light of the purpose of the above-mentioned system, for example, if a personal information handling business operator provides personal data to a third party in a foreign country based on a consent of a principal, the business operator is not required to take action, etc. under Article 24, paragraph 3 of the Act, even if the third party is deemed to have a system that conforms to the standards. (*) The stipulation of Article 24, paragraph 3 of the Act will apply to cases in which a personal information handling business operator provides personal data to a third party located in a foreign country as prescribed in the same paragraph on or after the effective date of Act revised in 2020 (Article 4, paragraph 2 of the Supplementary Provisions of the Act amended in 2020). 6-1 Necessary action to ensure the continuous implementation of equivalent action (related to Article 11-4, paragraph 1 of Commission Rules) When personal information handling business operator provides personal data to a third party located in a foreign country on the basis that the recipient has established a system that conforms to the standards, they must take the following action as necessary action to ensure the continuous implementation of equivalent action by the said third party. (1) Periodic confirmation, in an appropriate and reasonable manner, of the implementation status of the equivalent action by the third party, as well as the existence or non-existence of a system in said foreign country that may affect the implementation of said equivalent action, and the details thereof (related to Article 11-4, paragraph 1, item (i) of Commission Rules). Personal information handling business operator must periodically confirm, in an appropriate and reasonable manner, the implementation status of equivalent action by a third party recipient in a foreign country, as well as the existence or non-existence of a system in the said foreign country that may affect the implementation of the said equivalent action, and the details thereof. The term "periodically confirm" here means to confirm in a frequency of about once a year or more. The status of implementation of equivalent action must be confirmed by an appropriate and reasonable method depending on the content and scale of the personal data provided to a third party located in a foreign country. For example, the status may be confirmed by visiting the location where the personal data is handled, by receiving a written report, or by any other reasonable alternative method (including verbal confirmation). (*) [Examples applicable to the confirmation of the implementation status of equivalent action] Example 1) In the case of entrusting the handling of personal data to a business operator located in a foreign country, if the said business operator has established a system that conforms to the standards by concluding a contract between the provider and the recipient, the implementation status of the contract shall be confirmed. Example 2) In the case of a transfer of personal data within the same corporate group, if a privacy policy that is commonly applied to the provider and the recipient is used to establish a system that conforms to the standards by the recipient, the implementation of the privacy policy shall be confirmed.	

Title	Types of Data Covered	Selected Rules in Japan on Cross-Border Data Transfers or Data Localization	Sources
		The existence or non-existence of a system in a foreign country that may affect the implementation of equivalent action by a third party in a foreign country and its contents should be confirmed by an appropriate and reasonable method with general attention. For example, an inquiry may be made to the said third party, or information published by an administrative agency in Japan or a foreign country may be checked. [Examples falling as a system that may affect the implementation of equivalent action] Example 1) A system that allows the government to collect a wide range of information on personal information held by businesses operators by imposing on businesses operators an obligation to cooperate extensively with government information collection activities. Example 2) A system pertaining to the obligation to preserve personal information in the country which may not enable business operators to respond to a request for deletion, etc. from a principal. (*) Since the subject of the implementation of equivalent action by the third party recipient in a foreign country is the "personal data" actually provided by the personal information handling business operator, the confirmation of the implementation status of equivalent action does not require confirmation of the handling of other personal information handled by the third party recipient. (2) If an obstacle arises in the implementation of the equivalent action by the third party, necessary and appropriate action shall be taken, and if it becomes difficult to ensure the continuous implementation of the equivalent action, the provision of personal data to the said third party shall be suspended (related to Article 11-4, paragraph 1, item (ii) of Commission Rules). [Example applicable to necessary and appropriate action in case of an obstacle arising] Example) In the case in which a personal information handling business operator in Japan, by concluding a entrustment contract with a recipient business operator in a foreign country, established the system of the recipient business operator to conform to the standards, and the said business operator handles personal data in violation of some of the obligations under the said entrustment contract, the provider business operator requests to correct the situation. In addition, in the event that it becomes difficult to ensure the continuous implementation of equivalent action by a third party located in a foreign country, the provision to the said third party must be suspended thereafter, as the third party is considered, in effect, to not have established a system that conforms to the standards. [Examples in which it becomes difficult to ensure the continuous implementation of equivalent action] Example 1) In the case in which a personal information handling business operator in Japan, by concluding a consignment contract with a recipient business operator in a foreign country, established the system of the recipient business operator to conform to the standards, and the said business operator handles personal data in violation of some of the obligations under the said consignment contract, and despite the provider business operator requesting to correct the situation, the said recipient does not correct within the reasonable period. Example 2) After occurrence of a serious leakage, etc. of personal data provided by a personal information handling business operator in Japan at a business operator located in a foreign country, a necessary and appropriate preventive action to prevent a similar leakage, etc. is not taken by the recipient.	
PPC Explanation of the Draft Guidelines for the Act on the Protection of Personal Information (APPI), amended in 2020	Personal	[Enriching Information Regarding Cross-Border Transfer] -When transferring personal data to a third party in a foreign country, a business operator will be required to enrich the information provided to the principal regarding the handling of personal information at a recipient business operator. Post-APPI Amendment: The following will be obligated per the requirement based on each transfer: → provide the following at the time of obtaining consent from a principal (Article 24 (2) of APPI) • the name of the foreign country in which the recipient is located • the personal information protection system in the said foreign country • the action taken by the recipient to protect personal information → 1) the provider will be required to take the below ‘necessary action’: • periodic confirmation on the status of the appropriate handling by the recipient • response in the case of a problem arising on the appropriate handling by the recipient 2) upon request from a principal, provide information on ‘necessary action’ taken (Article 24 (3) of APPI) **Q. What is the level of detail required regarding the "system relating to the protection of personal information in the said foreign country"?**	PPC’s Explanation re Third Country Transfers under the Draft Guidelines for the Act on the Protection of Personal Information (APPI) (PDF)

Title	Types of Data Covered	Selected Rules in Japan on Cross-Border Data Transfers or Data Localization	Sources
		An exhaustive investigation is not required for the "systems relating to the protection of personal information in the said foreign country". However, for the purpose of increasing the predictability of a principal, it is necessary to provide information that enables reasonable recognition of the essential differences from Japan's personal information protection law, and specifically, the following points (1) through (4) should be taken into consideration: (1) existence or non-existence of a system for the protection of personal information in the recipient country (2) existence or non-existence of information that can be serve as an indicator of the system for protection of personal information in the recipient country (example: the country is a member of the APEC Cross-border Privacy Rules (CBPR), or a country that has obtained adequacy determination under Article 45 of the GDPR, etc.) (3) non-Existence of obligations by the business operator to respond to 8 principles of the OECD Privacy Guidelines (example: non-existence of restriction that, in principle, the personal information shall be used within the scope of the pre-specified utilization purpose, non-existence of the right of a principal to request the disclosure of personal information retained by business operator, etc.) (4) existence of other systems that may have a significant impact on the rights and interests of a principal (example: a system that allows the government to collect a wide range of personal information held by business operators by imposing on business operators an obligation to cooperate extensively with the government information collection activities, a system pertaining to the obligation to preserve personal information within the country which may not enable business operators to respond to request for deletion, etc. from a principal, etc.) **Q. Regarding the "system for the protection of personal information in the said foreign country" if partially inaccurate information had been provided to a principal, will it be a violation of obligations?** It is considered sufficient if the information provided to a principal has been checked in an appropriate and reasonable manner with general attention. Examples of "appropriate and reasonable method": • inquiry to the third party recipient • refer to the information published by the governmental organizations of Japan or foreign countries, etc. **Q. Shouldn't the Personal Information Protection Commission publicly release information on "the systems for the protection of personal information in foreign countries"?** The Personal Information Protection Commission is also planning to compile and release a set of information on the system for the protection of personal information in foreign countries which could serve as a reference for business operators. **Q. What level of information is required to be provided in relation to the “action to be taken by the recipient to protect personal information”?** With regards to the "action to be taken by the recipient to protect personal information", in light of the purpose of the system to increase the predictability of a principal, it is necessary to provide information that enables a principal to reasonably recognize the essential differences from the action required of personal information handling business operators in Japan on the handling of personal data. Specifically, if the recipient does not take action corresponding to the 8 principles of the OECD Privacy Guidelines, it is necessary to provide information on the details of such action not taken. -Example of providing information on "action taken by the recipient to protect personal information”: • In the case in which part of the action required of personal information handling business operators in Japan for the handling of personal data is not taken by the recipient. (example: notification and public disclosure of utilization purpose): *“The recipient generally takes action equivalent as those require of personal information handling business operators in Japan for the handling of personal data, however, does not notify or publicly disclose utilization purpose of the acquired personal information.”*	

Title	Types of Data Covered	Selected Rules in Japan on Cross-Border Data Transfers or Data Localization	Sources
		Q. What should be done in cases in which the foreign country of the third party recipient cannot be specified or there is a possibility to be transferred to multiple countries? If, at the time of obtaining consent from a principal, the recipient foreign countries can be specified, information on the systems in all foreign countries must be provided to a principal. However, in cases in which the recipient foreign countries cannot be specified at the time of obtaining consent from a principal, it is sufficient to provide the principal with information to that effect and the reasons therefor. However, even if the recipient foreign country cannot be specified, if it is possible to provide information such as the scope of the foreign countries to which the transfer is to be made, which would be helpful to the principal in place of the name of the recipient foreign countries, such information should also be provided to the principal. **Q. Regarding the provision of information to a principal, is it acceptable to post the information on the website of the personal information handling business operator that is the provider?** For example, when obtaining consent from a principal to allow the provision to a third party located in a foreign country, as stipulated in Article 24, paragraph 1 of APPI, it is considered acceptable to display the information to be provided to a principal on the screen on the website of the company transferring personal information as a means of providing information to a principal. **Q. In the case of cross-border transfer of personal data to a business operator that has established a system that conforms to the standards, what is required of the personal information handling business operator that is the provider for "periodic confirmation of the implementation status of the proper handling by the recipient"?** In the case in which a cross-border transfer of personal data is carried out based on the recipient establishing a system the conforms to the standards, the provider must confirm the following once a year or more, in an appropriate and reasonable manner: • Status of implementation of the appropriate handling of the said personal data by the recipient: (example: in the case of establishing the system of the recipient through entrustment contract between the provider and the recipient: the status of compliance of the said entrustment contract) • Existence or non-existence and details of a system that may affect the implementation of the appropriate handling in the country in which the recipient is located: (example: a system that allows the government to collect a wide range of personal information held by business operators by imposing on business operators an obligation to cooperate extensively with the government information collection activities, a system pertaining to the obligation to preserve personal information within the country which may not enable business operators to respond to request for deletion, etc. from a principal, etc.) Examples of confirmation in an appropriate and reasonable manner: • Receiving written report from the third-parity recipient, etc. **Q. In the case of a cross-border transfer of personal data to a business operator that has established a system that conforms to the standards, what is required of the personal information handling business operator that has transferred personal data to “respond to a problem arising in the appropriate handling of personal information at the recipient”?** In the case of a problem arising with the appropriate handling of personal data by the recipient, it is necessary to take necessary and appropriate measures to resolve the problem. Examples of necessary and appropriate action:	

Title	Types of Data Covered	Selected Rules in Japan on Cross-Border Data Transfers or Data Localization	Sources
		• In the case of concluding entrustment contract between the provider and the recipient and the recipient third party handles personal data in violation of the contract, request correction to be made, etc. Also, in the event that it becomes difficult to ensure the continuous implementation of appropriate handling by the recipient, it will be necessary to suspend the provision of personal data to the recipient thereafter. Examples of cases in which it has become difficult to ensure the continuous implementation of appropriate handling by the recipient: • In the case of concluding entrustment contract between the provider and the recipient and the recipient third party handles personal data in violation of the contract, and despite request to correct the situation, the recipient does not correct within reasonable period. • After the occurrence of a serious leakage etc. of personal data provided by personal information business operator in Japan at a business operator in a foreign country, a necessary and appropriate prevention action to prevent similar leakage etc. is not taken by the recipient. **Q. What kind of information regarding "necessary action" needs to be provided in response to a request from a principal?** Upon receiving a request from a principal, the provider must provide, for example, the below information regarding "necessary action" taken to ensure the continuous implementation of appropriate handling by the third party recipient. Example of provision of information regarding "necessary action" (in the case of provision of personal data to a third party located in country A as part of entrustment): • The method of establishment of the system that conforms to the standards: *Contract with the recipient* • Outline of equivalent action taken by the recipient: *In the case of handling personal data based on the agreement with recipient, provide information to the effect that personal data will be handlined within the specified utilization purpose, that inappropriate utilization is prohibited, that necessary and appropriate safety control action will be taken, that necessary and appropriate supervision will exercised over employees, that sub-contracting will be prohibited, that in the event of leakage, etc., the provider will report to the Personal Information Protection Commission and notify the principal, that third party provision of personal data is prohibited, etc.* • Name of the foreign country in which the third party recipient is located: *Country A* • The system in the foreign country that may affect the implementation of equivalent action to be taken by recipient: *There is a system that enables the government to collect a wide range of information on personal information retained by business operators by imposing a broad obligation on business operators to cooperate in the government's information collection activities.* • The frequency and method of confirmation: *Confirmation is done by receiving a written report from the recipient every year.* • Action to be taken in the case of obstacle arising in the implementation of equivalent action taken by the recipient: *The provision of personal data has been suspended due to the failure of the recipient to comply with contractual obligations and the difficulty in ensuring the continuous implementation of appropriate action*.	

Kazakhstan

Title	Types of Data Covered	Selected Rules in Kazakhstan on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The main legal act regulating personal data in Kazakhstan is the law of the Republic of Kazakhstan No. 94-V dated May 21, 2013 'On Personal Data and Its Protection' (the 'Law'). There are also a number of other laws providing for personal data protection requirements, including The Law on Informatisation; The Law on Communication; The Labour Code of Kazakhstan. Transfers of personal data are allowed if they do not violate the rights and freedoms of a personal data subject and do not affect the legitimate interests of other individuals and / or legal entities. The transfer of personal data in cases that go beyond the previously stated purposes of its collection is permitted if carried out with the consent of a personal data subject or his / her legal representative. The cross-border transfer of personal data to other countries is carried out only in cases where such countries ensure protection of personal data. The cross-border transfer of personal data to countries that do not ensure protection of personal data is possible: • With the consent of the personal data subject or his / her legal representative to the cross-border transfer of his / her personal data; • In cases stipulated by international treaties ratified by Kazakhstan; • In cases provided for by Kazakh law, if it is necessary for protecting the constitutional system, public order and public health and morals and rights and the freedoms of a person in Kazakhstan; • In case of protection of constitutional rights and freedoms of a person, if obtaining the consent of a personal data subject or his / her legal representative is impossible. *Kazakh law may in certain cases prohibit the cross-border transfer of personal data. See below*	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=KZ
On Personal Data and their Protection, The Law of the Republic of Kazakhstan dated 21 May, 2013 No. 94-V.	Personal	Excerpt **Article 16**. Trans-border transfer of personal data 1. Trans-border transfer of personal data – a transfer of personal data to the territory of the foreign states. 2. Trans-border transfer of personal data to the territory of the foreign states shall be carried out only in the case of ensuring of protection of personal data by these states in accordance with this Law. 3. Trans-border transfer of personal data to the territory of the foreign states, not ensuring protection of personal data may be carried out in the cases of: 1) existence of the consent of subject or his (her) legal representative to the trans-border transfer of his (her) personal data; 2) provided international treaties, ratified by the Republic of Kazakhstan; 3) provided by the Laws of the Republic of Kazakhstan, if it is necessary for the purposes of protection of constitutional order, protection of public order, rights and freedoms of person and citizen, health and morals of population; 4) protection of constitutional rights and freedoms of person and citizen, if reception of the consent of subject or his (her) legal representative is impossible. 4. Trans-border transfer of personal data to the territory of the foreign states may be prohibited or restricted by the Laws of the Republic of Kazakhstan. 5. Specifics for trans-border transfer of service information about subscribers and (or) users of communication services shall be determined by the Law of the Republic of Kazakhstan "On Communications". Footnote. Article 16 as amended by the Law of the Republic of Kazakhstan dated 28.12.2017 No. 128-VI (shall be enforced upon expiry of ten calendar days after its first official publication).	https://adilet.zan.kz/eng/docs/Z1300000094

Title	Types of Data Covered	Selected Rules in Kazakhstan on Cross-Border Data Transfers or Data Localization	Sources
The Law of the Republic of Kazakhstan No. 399-VI (January 2, 2021), Legislative Amendments (January 16, 2021)	Personal	Summary: Storage of personal data in electronic databases should be carried out in a server room on the territory of Kazakhstan.	Dentons, Kazakhstan strengthens personal data protection by gradually moving toward GDPR standards
Legislative Amendments of November 24, 2015 (No. 419-V) to the Kazakhstan Personal Data Protection Law (No. 94-V)	Personal	Excerpt: "**Article 12**: Accumulation and Storage of Personal Data 1. Accumulation of personal data shall be carried out by collecting personal data, necessary and sufficient to accomplish the tasks carried out by the owner and / or operator, as well as by a third party. 2. Storage of personal data shall be carried out by the owner and/ or operator, as well as by a third party in the database, which is kept in the territory of the Republic of Kazakhstan."	Kazakhstan, Law of Kazakhstan on Personal Data and its Protection (as amended) MorganLewis, Data Localization Laws of Kazakhstan DAC Beachcroft, Kazakhstan – Localization of personal data
Communications Law of the Republic of Kazakhstan dated 28.12.2017 No. 128-VI	Personal	Excerpt: "Preamble: This Law establishes legal grounds for activity in the field of communications in the territory of the Republic of Kazakhstan, determines the powers of state bodies on regulation of this activity, right and obligation of individuals and legal entities rendering or using the services of communications. **Article 15(2):** Storage of official information about the subscribers shall be carried out exclusively on the territory of the Republic of Kazakhstan. It is forbidden to transfer official information about the subscribers outside the Republic of Kazakhstan, except for the cases of provision of communication services to the subscribers of the Republic of Kazakhstan located abroad."	Kazakhstan, Law of the Republic of Kazakhstan dated 28.12.2017 No. 128-VI MorganLewis, Data Localization Laws of Kazakhstan
Law on Informatization - Law of the Republic of Kazakhstan dated 24 November 2015 № 418-V.	Various	Excerpt: 2-1. Information system of a state legal entity and non-state information system intended for formation of state electronic information resources shall be created, operated and developed in accordance with the legislation of the Republic of Kazakhstan,standards, operating on the territory of the Republic of Kazakhstan, the life cycle of the information system and provided that the following requirements are performed: … 3. The information contained in the electronic information resource, normative and technical documentation, as well as other related documents of the information system of state bodies are created and stored in Kazakh and Russian languages. 4. The owner or the possessor of information system of the state body or the person authorized by him after its introduction into industrial operation shall provide to the National coordination center for information security the access to the information system of the state body at its location for conducting monitoring of information security ensuring.	Kazakhstan, Law on Informatization - Law of the Republic of Kazakhstan dated 24 November 2015 № 418-V MorganLewis, Data Localization

Title	Types of Data Covered	Selected Rules in Kazakhstan on Cross-Border Data Transfers or Data Localization	Sources
			Laws of Kazakhstan
Order No. 38/NK of the Minister for Defense and Aerospace Industry of the Republic of Kazakhstan ("On the Approval of the Rules for Registration, Use, and Distribution of Domain Names in the Area of Kazakhstani Segment of the Internet") (as amended on March 13, 2018) (Order No. 38/NK)	Various	Summary: Order No. 38/NK governs the procedures for registering domain names in the Kazakhstani segment of the internet, defined as set of internet sites hosted on hardware and software located in the Republic of Kazakhstan (Paragraph 2(5), Order 38/NK). The domain registration application contains a provision requiring server hardware to be located in the Republic of Kazakhstan (see Note, Appendix to the Rules for Registration, Use, and Distribution to the Kazakhstani Segment of the Internet)	Kazakhstan,Order No. 38/NK on the Approval of the Rules for Registration, Use, and Distribution of Domain Names MorganLewis, Data Localization Laws of Kazakhstan
Resolution of the Government of the Republic of Kazakhstan dated 28.04.2018 No. 229	Various	Excerpt: "6-1. Storage of service information about subscribers shall be carried out exclusively in the territory of the Republic of Kazakhstan. Transfer of service information about subscribers outside the Republic of Kazakhstan shall be prohibited, except for cases of rendering communication services to subscribers of the Republic of Kazakhstan located abroad."	Kazakhstan, Resolution of the Government of the Republic of Kazakhstan dated 28.04.2018 No. 229 MorganLewis, Data Localization Laws of Kazakhstan

Korea (Republic of Korea)

Title	Types of Data Covered	Selected Rules in Republic of Korea on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The Korean legislative system for personal information protection is composed of the Personal Information Protection Act ("**PIPA**"), a general, comprehensive statute and the Credit Information Use and Protection Act which regulates personal credit information. As a general rule, a personal data controller may not provide personal information to a third party without obtaining the prior opt in consent of the data subject. Exceptions to the general rule above apply in the following cases: • where there exist special provisions in any Act or it is necessary to fulfil an obligation imposed by or under any Act and subordinate statute • where it is necessary for a public institution to perform its affairs provided for in any Act and subordinate statute, etc, and • where it is deemed obviously necessary for the physical safety and property interests of a data subject or a third person when the data subject or his/her legal representative cannot give prior consent because he/she is unable to express his/her intention or by reason of his/her unidentified address, etc. Under the PIPA, a personal data controller must obtain consent after it notifies the data subject of: • the person (entity) to whom the personal information is furnished • purpose of use of the personal information by the person (entity) • types of personal information furnished • period of time during which the person (entity) will possess and use the personal information, and • the fact that the data subject has the right to refuse to consent and the consequences of refusing. While there is no additional requirement for the personal data controller other than the general requirements for third party transfer described above, there is a special provision for cross-border transfer of personal information of "Users" (which is defined as all individuals who use the telecommunications services provided by Online Service Providers). If a User's personal information is transferred to an overseas entity, Online Service Providers must disclose and obtain the User's consent with respect to the following: • the specific information to be transferred overseas • the destination country • the date, time, and method of transmission • the name of the third party and the contact information of the person in charge of the personal information within the third party, and • the third party's purpose of use of the personal information and the period of retention and usage. In principle, this requirement applies irrespective of whether the transfer constitutes a provision of personal information to a third party or an outsourcing of personal information processing, provided that the obligation to obtain Users' consent may be exempted for outsourcing of personal information processing or storage of personal information if the aforementioned items are disclosed in the privacy policy. Under the PIPA, when processing personal information acquired indirectly by way of a third party transfer, transferees who meet a certain threshold as provided by the Presidential Decree will be obligated to notify the data subject of (i) the third party source (transferor) from which the personal information was acquired, (ii) the intended use of the received personal information, and (iii) the fact that the data subject has the right to request for suspension from processing personal information.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=KR
PERSONAL INFORMATION PROTECTION ACT [Enforcement Date 05. Aug, 2020.] [Act No.16930, 04.	Personal	Excerpt (machine translated) **Article 14** (International Cooperation) (1) The Government shall establish policy measures necessary to enhance the personal information protection standard in the international environment. (2) The Government shall establish relevant policy measures so that the rights of data subjects may not be infringed on owing to the cross-border transfer of personal information.	https://www.law.go.kr/LSW/eng/engLsSc.do?y=0&x=0&menuId=2&query=personal+&section=lawNm#liBgcolor1

Title	Types of Data Covered	Selected Rules in Republic of Korea on Cross-Border Data Transfers or Data Localization	Sources
Feb, 2020., Partial Amendment]		**Article 17** (Provision of Personal Information) (1) A personal information controller may provide (or share; hereinafter the same shall apply) the personal information of a data subject to a third party in any of the following circumstances: <Amended by Act No 16930, February. 4, 2020> 1. Where the consent is obtained from the data subject; 2. Where the personal information is provided within the scope of purposes for which it is collected pursuant to Articles 15 (1) 2, 3 and 5 and 39-3 (2) 2 and 3. (2) A personal information controller shall inform a data subject of the following matters when it obtains the consent under paragraph (1) 1. The same shall apply when any of the following is modified: 1. The recipient of personal information; 2. The purpose for which the recipient of personal information uses such information; 3. Particulars of personal information to be provided; 4. The period during which the recipient retains and uses personal information; 5. The fact that the data subject is entitled to deny consent, and disadvantages, if any, resulting from the denial of consent. (3) A personal information controller shall inform a data subject of the matters provided for in paragraph (2), and obtain the consent from the data subject in order to provide personal information to a third party overseas; and shall not enter into a contract for the cross-border transfer of personal information in violation of this Act. (4) A personal information controller may provide personal information without the consent of a data subject within the scope reasonably related to the purposes for which the personal information was initially collected, in accordance with the matters prescribed by Presidential Decree taking into consideration whether disadvantages are caused to the data subject, whether necessary measures to secure safety, such as encryption, have been taken, etc. **Article 39-12** (Protection of Information Transferred Overseas) (1) The information and communications service provider, etc. shall not execute an international contract in violation of this Act in relation to users' personal information. (2) Notwithstanding Article 17 (3), information and communications service provider, etc. shall obtain users' consent if intending to provide (including accessing), outsource the processing of, or store (hereinafter referred to as "transfer" in this Article) users' personal information overseas: Provided, That if all items of paragraph (3) below are made public pursuant to Article 30 (2) or notified to users by a method prescribed by the Presidential Decree such as e-mail, the information and communications service provider, etc. may opt not to obtain users' consent to outsourcing the processing of, or storing, personal information. (3) The information and communications service provider, etc. shall notify users of the following matters in advance if intending to obtain consent under paragraph (2): 1. Particulars of the personal information to be transferred; 2. The country to which the personal information is transferred, transfer date and method; 3. Name of the entity to which the personal information is transferred (referring to the name of a corporation and the contact information of the person responsible for the management of information, if the person is a corporation); 4. The purpose of using personal information by the entity to which the information is transferred and the period of retaining and using personal information. (4) The information and communications service provider, etc. shall implement safeguards as prescribed by Presidential Decree if intending to transfer personal information overseas with consent obtained pursuant to paragraph (2). (5) where a person who receives personal information of the users transfers it to a third country, he or she shall comply with paragraphs (1) through (4). In such cases, "information and communications service providers, etc." shall be regarded as "personal information recipient," and "personal information recipient" shall be regarded as "a person who receives personal information from a third country. **Article 39-13** (Reciprocity)	

Title	Types of Data Covered	Selected Rules in Republic of Korea on Cross-Border Data Transfers or Data Localization	Sources
		Notwithstanding Article 39-12, information and communications service providers, etc. in a country that restricts cross-border transfer may face an equivalent level of restrictions in another country: Provided, That this shall not apply where cross-border transfer is necessary to implement a pact or other international arrangements.	
ENFORCEMENT DECREE OF THE PERSONAL INFORMATION PROTECTION ACT [Enforcement Date 05. Aug, 2020.] [Presidential Decree No.30892, 04. Aug, 2020., Partial Amendment]	Personal	Excerpt (machine translated) **Article 48-10** (Safeguards in the Event of Overseas Transfer of Personal Information) (1) If any Information and Communications Service Provider, etc. intends to transfer personal information overseas in accordance with the main clause of Article 39-12 (2) of the Act, it shall implement the following safeguards according to paragraph (4) of the same Article: 1. Measures to ensure safety for protection of personal information in accordance with Article 48-2 (1); 2. Matters concerning handling of complaints and dispute resolution concerning infringement with respect to personal information; 3. Other measures necessary to protect users' personal information. (2) If any Information and Communications Service Provider, etc. intends to transfer personal information overseas in accordance with the main clause of Article 39-12 (2) of the Act, the Information and Communications Service Provider, etc. shall discuss each subparagraph of paragraph (1) with the recipient in advance and incorporate the same into the terms of the agreement. (3) The "method prescribed by Presidential Decree such as e-mail" in the proviso of Article 39-12 (2) of the Act means written notice, etc.	https://www.law.go.kr/LSW/eng/engLsSc.do?y=0&x=0&menuId=2&query=personal+&section=lawNm#liBgcolor0

Kenya

Title	Types of Data Covered	Selected Rules in Kenya on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The Data Protection Act, 2019 (the "**Act**") came into force on 25th November, 2019 and is now the primary statute on data protection in Kenya. It gives effect to Article 31 c) and d) of the Constitution of Kenya, 2010 (right to privacy). In October 2020, by virtue of the powers conferred to him under the Act, the Cabinet Secretary for Information, Communication, Technology, Innovation and Youth Affairs gazetted the Data Protection (Civil Registration) Regulations, 2020 (the "**Regulations**"). The Regulations apply to civil registries involved in processing personal data for registrations such as births, deaths, adoptions, persons, passports and marriages. Since the Data Protection Commissioner's (DPC) appointment on 16 November 2020, significant efforts have been made in developing regulations for the implementation of the Act. • **Data Protection (Compliance & Enforcement) Regulation, 2021** – sets out the complaints handling procedures and enforcement mechanisms in the event of non-compliance with the provisions of the Act; • **Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021** – provides for the registration of data controllers and data processors with the DPC. The threshold for mandatory registration is also set out under these regulations; and • **Data Protection (General) Regulations, 2021** – elaborates in more detail the rights of data subjects, restrictions on commercial use of personal data, duties and obligations of data controllers and data processors, elements of implementing data protection by design or default, notification of personal data breaches, transfer of personal data outside Kenya, conduct of data protection impact assessment and other general provisions. Part VI of the Act The transfer of personal data outside Kenya is highly regulated under the Act. Prior to any transfer the data controller or data processor must provide proof to the DPC on the appropriate safeguards with respect to the security and protection of the personal data including jurisdictions with similar data protection laws. The consent of the data subject is required for the transfer of sensitive personal data out of Kenya. Under the Regulations, civil registration registries cannot transfer personal data collected for civil registration purposes outside Kenya without the written approval of the DPC. **The Data Protection (General) Regulations, 2021** elaborate in more detail transfer of personal data outside Kenya. However, the regulations are yet to be passed into law and are currently awaiting signature by the CS after which they shall be published in the Kenya Gazette.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=KE
Data Protection General Regulations, 2020	Personal	Excerpt **Article 25:** "(1) Pursuant to section 50 of the Act, a data controller or data processor who processes personal data for the purpose of actualising a public good set out under paragraph (2) shall be required to ensure that— (a) such processing is effected through a server and data centre located in Kenya; and (b) at least one serving copy of the concerned personal data is stored in a data centre located in Kenya. (2) The purpose contemplated under paragraph (1) that require processing in Kenya includes— (a) administering a national civil registration system including registrations of births and deaths, persons, adoption and marriages; (b) operating a population register and identity management system including any issuance of any public document of identity; (c) managing personal data to facilitate access of primary and secondary education in the country; (d) the conduct of elections in the country; (e) managing any electronic payments systems licensed under the National Payment Systems Act; (f) any revenue administration system for public finances; (g) processing health data for any other purpose other than providing health care directly to a data subject; or (h) managing any system designated as a protected computer system in terms of section 20 of the Computer Misuse and Cybercrime Act, 2018. (3) Despite paragraph (2), the Cabinet Secretary may require a data controller who processes personal data outside Kenya to comply with paragraph (1), if the data controller—	Kenya, Data Protection General Regulations, 2020

Title	Types of Data Covered	Selected Rules in Kenya on Cross-Border Data Transfers or Data Localization	Sources
		(a) has been notified that personal data outside Kenya has been breached or its services have been used to violate the Act and has not taken measures to stop or handle the violation; and (b) resists, obstructs or fails to comply with requests of the Data Commissioner or any other relevant authority in— (i) cooperating to investigate and handle such violations; or (ii) neutralize and disable the effect of cyber security protection measures."	
The Data Protection Act, 2019 (Kenya Gazette Supplement No. 181 (Acts No. 24))	Personal	Excerpt **PART VI** —TRANSFER OF PERSONAL DATA OUTSIDE KENYA **Conditions for transfer out of Kenya** **48.** A data controller or data processor may transfer personal data to another country only where — (a) the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data; (b) the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws; (c) the transfer is necessary — (i) for the performance of a contract between the data subject and the data controller or data processor or implementation of precontractual measures taken at the data subject's request; (ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person; (iii) for any matter of public interest; (iv) for the establishment, exercise or defence of a legal claim; (v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or (vi) for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects. Safeguards prior to transfer of personal data out of Kenya **49**. (1) The processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards. (2) The Data Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the security safeguards or the existence of compelling legitimate interests. (3) The Data Commissioner may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as may be determined. Processing through a data server or data centre in Kenya. **50.** The Cabinet Secretary may prescribe, based on grounds of strategic interests of the state or protection of revenue, certain nature of processing that shall only be effected through a server or a data centre located in Kenya.	http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf

Kyrgyzstan

Title	Types of Data Covered	Selected Rules in Kyrgyzstan on Cross-Border Data Transfers or Data Localization	Sources
THE LAW OF THE KYRGYZ REPUBLIC On Personal Data (14th of April 2008 N 58)	Personal	Excerpt Articles 3. Terms and definitions Transfer of the personal data - the personal data communication by its holder to third parties in conformity with the present law and the international treaties. Transboundary transfer of the personal data - the personal data communication by its holder to the holders being under jurisdiction of other states. Article 24. Transfer of the personal data 1. The holder (owner) of the personal data file shall have the right to transfer these data to other holder (owner) without the personal data subject's consent in cases:emergency for protection of the personal data subject's vital interests; of inquiry of the state power bodies, local state administrations, local self-government bodies if the required list of the personal data corresponds to the powers of the requesting body; in pursuance with the law. 2. The holder (owner) of the personal data files is obliged to inform the subject of the personal data concerning transmission of his personal data to the third side in any form withing the week period. 3. When transferring the personal data the recipient shall be liable for confidentiality mode observance relating to these data. 4. The personal data collected at the expenses of the state budget funds, shall be transferred free-of-charge to the bodies of the state power and organizations of budgetary sphere. Article 25. Transboundary transfer of the personal data 1. At transboundary transfer of the personal data, the holder (owner) of the personal data file, located under the jurisdiction of the Kyrgyz Republic and transferring the data, shall proceed from the international treaty between the parties according to which the receiving party shall provide level of protection of rights and freedoms of the personal data subjects and the personal data security equal to that of established in the Kyrgyz Republic. 2. The Kyrgyz Republic provides legal protection measures for the personal data located in its territory or transferred through its territory, precluding their distortion and unauthorized use. 3. Transfer of the personal data files by the holders (owners), located within jurisdiction of the Kyrgyz Republic, to the countries which are not providing level of protection of rights and freedoms of the personal data subjects equal to that of existing in the Kyrgyz Republic, may take place provided that: - The obviously expressed consent of the personal data subject to this transfer; - If the transfer is necessary for protection of the personal data subject's vital interests; - If the personal data are contained in the generally accessible personal data file. 4. Where transferring the personal data through the global information network (the Internet, etc.) the holder (owner) of the personal data file, transferring such data, shall be obliged to provide the necessary security means for such transfer, including confidentiality.	https://www.legislationline.org/download/id/4220/file/Kyrgyz_Law_personal_data_2008_EN.pdf

Title	Types of Data Covered	Selected Rules in Latvia on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	See Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Lesotho

Title	Types of Data Covered	Selected Rules in Lesotho on Cross-Border Data Transfers or Data Localization	Sources
Data Protection Act, 2011 (ACT NO. 5 OF ZO12)	Personal	Excerpt Transfer of personal information outside Lesotho **52.** A data controller in Lesotho shall not transfer personal information about a data subject to a third party who is in a foreign country unless: (a) the recipient of the information is subject to a law, code of conduct or. contract which (i) effectively uphoids principles for reasonable processing of the information that are substantially similar to the information protection principles under this Act; and (ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country; (b) the data subject consents to the transfer; (c) the transfer is necessary for the performance of a contract between the data subject and the data controller, or for the implementation of pre-contractual measures taken in response to the data subject's request; (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data contloiler and a third party; or (e) the transfer is for the benefit of the data subject and - (i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; or (ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.	http://www.nic.ls/lsnic/community/policies/Data_Protection_Act_2011_Lesotho.pdf

Liechtenstein

Title	Types of Data Covered	Selected Rules in Liechtenstein on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Lithuania

Title	Types of Data Covered	Selected Rules in Lithuania on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Luxembourg

Title	Types of Data Covered	Selected Rules in Luxembourg on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Macedonia

Title	Types of Data Covered	Selected Rules in The former Yugoslav Republic of Macedonia on Cross-Border Data Transfers or Data Localization	Sources
Of the Law on personal data protection	Personal	Excerpt III.TRANSFER OF PERSONAL DATA COLLECTION TO OTHER STATES 1. Transfer of personal data Collections out of state borders **Article 15** The transfer of personal data Collection to other states may be performed only in accordance to the legally prescript procedure and only if that other state has the same protection measures for the personal data Collections. The transferred data form the personal data Collection may be used only for the purposes for which the transfer has been performed. **Article 16** The estimation of whether that other state applies the same protection measures to the personal data Collection shall be done in accordance to the conditions under which the transfer of the already processed personal data Collection is performed, or the conditions under which the transfer of the personal data Collection to be processed is performed. While estimating the oneness of the protection measures applied to the personal data Collection, special consideration shall be put on he nature of the personal data Collection which is to be transferred, the aims and the length of the processing operations in the state to which the personal data Collection is to be transferred and especially to the legal provisions regulating the personal data Collections in that particular state. The oneness of the provisions applied for protection of personal data in other state shall be estimated by the Personal Data Protection Directorate (further on in the text: Directorate). **Article 17** If the state to which the personal data Collection is to be transferred does not fulfill the conditions of its protection, the transfer shall not be performed. The Directorate may not allow a transfer of data from the personal data Collection even when there are adequate legal provisions for their protection in the other state in accordance to the law and to the ratified international agreement. **Article 18** The provisions of Article 17 of this Law shall not apply if: • The subject of the personal data Collection allows the transfer; • The transfer is needed for the purposes of fulfilling an agreement concluded between the subject of the personal data Collection and the Controller; • The transfer is needed for the purposes of fulfilling an agreement concluded between the subject of the personal data Collection, the Controller and third party; • The transfer is needed to protect the public interest or to protect the fundamental rights and freedoms of the citizens; • The transfer is needed to protect the vital interests of the subject of the personal data Collection. Except for the conditions determined in paragraph 1 of this Article, the Directorate may allow personal data Collection transfer to other state even when the provisions of that state do not provide sufficient level of their protection, if the Controller of the other state verifies the existence of sufficient protection measures as for the rights of privacy of his personal and family life.	https://www.legislationline.org/download/id/1247/file/22fb16d752a9b7737b6fc8252ba5.pdf

Title	Types of Data Covered	Selected Rules in Madagascar on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Law No. 2014-038 relating to protection of personal data is the main regulatory framework in Madagascar (the 'Data Protection Law'). After discussion at the National Assembly of Madagascar, the Data Protection Law was adopted on 16 December 2014. The Law was promulgated by the President of Republic of Madagascar on 9 January 2015. The transfer of a data subject's personal data to a third party country is allowed only if the country guarantees to individuals a sufficient level of protection in terms of privacy and fundamental rights and liberties. The sufficiency of the protection is assessed by considering all the circumstances surrounding the transfer, in particular the nature of the data, the purpose and the duration of the proposed processing, country of origin and country of final destination, rules of law, both general and sectorial in force in the country in question and any relevant codes of conduct or other rules and security measures which are complied with in that country. Data controllers may transfer personal data to a third country that is not deemed to offer adequate protection only if: • the data subject consents and duly informed of the absence of adequate protection • the transfer is necessary: o for the performance of a contract between the data controller and the individual, or pre-contractual measures undertaken at the individual's request o for the conclusion or the performance of a contract in the interest of the individual, between the data controller and a third party o for the protection of the public interest o for consultation of a public register intended for the public's information o to comply with obligations allowing the acknowledgment, the exercise or the defence of a legal right. In all cases, the data recipient in the third party country cannot transfer personal data to another country, except with the authorisation of the first data controller and the CMIL .	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=MG
Law No. 38/2014 Protection of personal data (in French)	Personal	Not excerpted or summarized due to lack of translation.	https://www.afapdp.org/wp-content/uploads/2015/01/Madagascar-L-2014-038-du-09-01-15-sur-la-protection-des-donn%c3%a9es-%c3%a0-caract%c3%a8re-personnel.pdf

Malaysia

Title	Types of Data Covered	Selected Rules in Malaysia on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Malaysia's first comprehensive personal data protection legislation, the Personal Data Protection Act 2010 (PDPA), was passed by the Malaysian Parliament on June 2, 2010 and came into force on November 15, 2013.Under the PDPA, a data user may not transfer personal data to jurisdictions outside of Malaysia unless that jurisdiction has been specified by the Minister. However, there are exceptions to this restriction, including the following: • The data subject has given his or her consent to the transfer. • The transfer is necessary for the performance of a contract between the data subject and the data user. • The data user has taken all reasonable steps and exercised all due diligence to ensure that the personal data will not be processed in a manner that would contravene the PDPA. • The transfer is necessary to protect the data subject's vital interests. In 2017, the Commissioner published a draft Personal Data Protection (Transfer of Personal Data to Places Outside Malaysia) Order 2017 to obtain public feedback on the proposed jurisdictions to which personal data from Malaysia may be transferred. As of December 15, 2020, the Minister has yet to approve the safe harbor jurisdictions. Once approved, a data user may transfer personal data to these safe harbor jurisdictions without having to rely on the data subject's consent or other prescribed exceptions under the PDPA. Pursuant to PC01/2020, the Commissioner acknowledged that a clear provision and the conditions for transferring personal data to places outside Malaysia are essential to facilitate e-commerce transactions and free trade agreements, and opined that a whitelist appears to curb and set a barrier for data users to transfer personal data to places outside Malaysia. In view of this, the Commissioner is considering restructuring the provision on cross border transfers under the PDPA and removing the whitelist provision. In addition, the Commissioner also acknowledged that data users with overseas branches may need to exchange information with its branches at some point. The Commissioner is considering issuing a guideline on the mechanism and implementation of cross border data transfer and has sought feedback on the important matters to be considered in the proposed guideline.	https://www.dlapiperdataprotection.com/index.html?t=law&c=MY
LAWS OF MALAYSIA Act 709 PERSONAL DATA PROTECTION ACT 2010	Personal	Excerpt PART X - MISCELLANEOUS Transfer of personal data to places outside Malaysia 129. (1) A data user shall not transfer any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Minister, upon the recommendation of the Commissioner, by notification published in the Gazette. (2) For the purposes of subsection (1), the Minister may specify any place outside Malaysia if— (a) there is in that place in force any law which is substantially similar to this Act, or that serves the same purposes as this Act; or (b) that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by this Act. (3) Notwithstanding subsection (1), a data user may transfer any personal data to a place outside Malaysia if— (a) the data subject has given his consent to the transfer;	https://www.dataguidance.com/sites/default/files/personal_data_protection_act_2010.pdf

Title	Types of Data Covered	Selected Rules in Malaysia on Cross-Border Data Transfers or Data Localization	Sources
		(b) the transfer is necessary for the performance of a contract between the data subject and the data user; (c) the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which— (i) is entered into at the request of the data subject; or (ii) is in the interests of the data subject; (d) the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights; (e) the data user has reasonable grounds for believing that in all circumstances of the case— (i) the transfer is for the avoidance or mitigation of adverse action against the data subject; (ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and (iii) if it was practicable to obtain such consent, the data subject would have given his consent; (f) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of this Act; (g) the transfer is necessary in order to protect the vital interests of the data subject; or (h) the transfer is necessary as being in the public interest in circumstances as determined by the Minister (4) Where the Commissioner has reasonable grounds for believing that in a place as specified under subsection (1) there is no longer in force any law which is substantially similar to this Act, or that serves the same purposes as this Act— (a) the Commissioner shall make such recommendations to the Minister who shall, either by cancelling or amending the notification made under subsection (1), cause that place to cease to be a place to which personal data may be transferred under this section; and (b) the data user shall cease to transfer any personal data of a data subject to such place with effect from the time as specified by the Minister in the notification. (5) A data user who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both. (6) For the purposes of this section, “adverse action”, in relation to a data subject, means any action that may adversely affect the data subject’s rights, benefits, privileges, obligations or interests	

Mali

Title	Types of Data Covered	Selected Rules in Mali on Cross-Border Data Transfers or Data Localization	Sources
Lois sur la protection des données à caractère personnel - Loi n° 2013-015 du 21 mai 2013 (in French)	Personal	Not excerpted or summarized due to lack of translation.	https://www.afapdp.org/wp-content/uploads/2012/01/Mali-Loi-sur-la-protection-des-donn%c3%a9es-personnelles-du-21-mai-2013.pdf

Malta

Title	Types of Data Covered	Selected Rules in Malta on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	*See* Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Mauritania

Title	Types of Data Covered	Selected Rules in Mauritania on Cross-Border Data Transfers or Data Localization	Sources
Loi 2017-020 sur la protection des données à caractère personnel	Personal	Not excerpted or summarized due to lack of translation.	https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/ContentRegulation/Mauritania_2.pdf

Mauritius

Title	Types of Data Covered	Selected Rules in Mauritius on Cross-Border Data Transfers or Data Localization	Sources
The Data Protection Act, 2017 Act No. 20 of 2017 Proclaimed by [Proclamation No. 3 of 2018] w.e.f. 15 January 2018 Government Gazette of Mauritius No. 120 of 23 December 2017	Personal	Excerpt **PART VI – TRANSFER OF PERSONAL DATA OUTSIDE MAURITIUS** **36.** Transfer of personal data outside Mauritius (1) A controller or processor may transfer personal data to another country where – (a) he or it has provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data; (b) the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer owing to the absence of appropriate safeguards; (c) the transfer is necessary – (i) for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (i) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person; (ii) for reasons of public interest as provided by law; (iv) for the establishment, exercise or defence of a legal claim; or (v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or (vi) for the purpose of compelling legitimate interests pursued by the controller or the processor which are not overridden by the interests, rights and freedoms of the data subjects involved and where – (A) the transfer is not repetitive and concerns a limited number of data subjects; and (B) the controller or processor has assessed all the circumstances surrounding the data transfer operation and has, based on such assessment, provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data; or (d) the transfer is made from a register which, according to law, is intended to provide information to the public and which is open for consultation by the public or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down by law for consultation are fulfilled in the particular case. (2) A transfer pursuant to subsection (1)(d) shall not involve the entirety of the personal data or entire categories of the personal data contained in the register and, where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or in case they are to be the recipients. (3) Subsection (1)(a) and (c)(i), (ii) and (vi) shall not apply to activities carried out by a public authority in the exercise of its functions. (4) The Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the safeguards or the existence of compelling legitimate interests and may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as he may determine.	https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/108724/134563/F686980207/MUS108724.pdf

Mexico

Title	Types of Data Covered	Selected Rules in Mexico on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Mexican privacy laws distinguish between 'transfers' of personal data (to third parties) and transmissions of personal data (to processors). Under Mexican Privacy Laws, a 'transfer' is any communication or transmission of personal data by or on behalf of the Controller to a third party (not including a processor). Where the data controller intends to transfer personal data to domestic or foreign third parties other than a data processor, it must provide the third parties with the privacy notice provided to the data subject and the purposes to which the data subject has limited the data processing. In addition, the controller must notify data subjects in the privacy notice of the transfer, including: • that the transfer may be made, as well as to whom and for what purposes the personal data may be transferred. • where consent to the transfer is required, that the data subject consents and how the data subject can refuse to consent to the relevant transfer(s). The purpose of the transfer must be limited to the purpose and conditions informed in the privacy notice and consented to by the data subject (as applicable). The third-party recipient must assume the same obligations as the data controller who has transferred the data. Domestic and international transfers of personal data may be carried out without the consent of the data subject where the transfer is: • Pursuant to a law or treaty to which Mexico is party • Necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management • Made to the holding company, subsidiaries or affiliates under the common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies as the data controller (provided they will comply with principles of Mexican Privacy Laws, the privacy notice provided to data subjects and the other applicable internal policies regarding data protection) • Necessary by virtue of a contract executed or to be executed between the data controller and a third party in the interest of the data subject • Necessary or legally required to safeguard public interest or for the administration of justice • Necessary for the recognition, exercise or defense of a right in a judicial proceeding, or • Necessary to maintain or comply with an obligation resulting from a legal relationship between the data controller and the data subject The Regulations establish that communications or transmissions of personal data to processors do not need to be notified or consented to by the data subject. However, the data processor must do all of the following: • Process personal data only according to the instructions of the data controller • Not process personal data for a purpose other than as instructed by the data controller • Implement the security measures required by the Law, the Regulations and other applicable laws and regulations • Maintain the confidentiality of the personal data subject to processing • Delete personal data that were processed after the legal relationship with the data controller ends or when instructed by the data controller, unless there is a legal requirement for the preservation of the personal data • Not transfer personal data unless instructed by the data controller, the communication arises from subcontracting, or if so required by a competent authority	

Title	Types of Data Covered	Selected Rules in Mexico on Cross-Border Data Transfers or Data Localization	Sources
Federal Law on Protection of Personal Data Held by Private Parties (2010) (Ministry of Interior Decree) (Federal Official Gazette, dated July 5, 2010)	Personal	Excerpt **CHAPTER V - Data Transfer** **Article 36.** Where the data controller intends to transfer personal data to domestic or foreign third parties other than the data processor, it must provide them with the privacy notice and the purposes to which the data owner has limited data processing. Data processing will be done as agreed in the privacy notice, which shall contain a clause indicating whether or not the data owner agrees to the transfer of his data; moreover, the third party receiver will assume the same obligations as the data controller that has transferred the data. **Article 37.** Domestic or international transfers of data may be carried out without the consent of the data owner in the following cases: I. Where the transfer is pursuant to a Law or Treaty to which Mexico is party; II. Where the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management; III. Where the transfer is made to holding companies, subsidiaries or affiliates under common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies; IV. Where the transfer is necessary by virtue of a contract executed or to be executed in the interest of the data owner between the data controller and a third party; V. Where the transfer is necessary or legally required to safeguard public interest or for the administration of justice; VI. Where the transfer is necessary for the recognition, exercise or defense of a right in a judicial proceeding, and VII. Where the transfer is necessary to maintain or fulfill a legal relationship between the data controller and the data owner. **CHAPTER X** **Violations and Penalties** **Article 63.** The following acts carried out by the data controller are violations of this Law: X. Transferring data to third parties without providing them with the privacy notice containing the limitations to which the data owner has conditioned data disclosure; ... XII. Carrying out the transfer or assignment of personal data outside of the cases where it is permitted under this Law; XIII. Collecting or transferring personal data without the express consent of the data owner, in the cases where this is required;	Mexico Official Gazette, Federal Law on the Protection of Personal Data Held by Private Parties

Title	Types of Data Covered	Selected Rules in Mexico on Cross-Border Data Transfers or Data Localization	Sources
Regulations to the Federal Law on the Protection of Personal Data Held by Private Parties (Federal Official Gazette, dated Dec. 11, 2011)	Personal	Excerpt Chapter II - Principles of Protection of Personal Data Transmission of Personal Data Article 53. National and international transmissions of personal data between a data controller and a data processor need not be informed to the data subject or his consent obtained. The data processor shall be considered as a data controller, together with its own obligations, when it: I. Uses the personal data for a purpose different from that authorized by the data controller, or II. Makes a transfer without complying with the instructions of the data controller. The data processor will not be held responsible when, at the express indication of the data controller, it transmits the personal data to another data processor designated by the latter, to which it had entrusted the performance of a service, or transfers the personal data to another data controller pursuant to these Regulations. Chapter IV - Transfers of Personal Data Scope Article 67. A transfer refers to the communication of personal data to a person other than the data subject, data controller or data processor, within or outside Mexico. Conditions for a Transfer Article 68. Any transfer of personal data, whether national or international, is subject to the consent of the data subject, with the exceptions provided in Article 37 of the Law; the data subject must be so informed by a privacy notice and the transfer be limited to the purposes that justify it. Proof of Compliance with Transfer Obligations Article 69. For purposes of demonstrating that the transfer, whether national or international, took place in accordance with the Law and these Regulations, the burden of proof in all cases rests upon the data controller that made the transfer and on the receiver of the personal data. Transfers within the Data Controller's Group Article 70. In the case of transfers of personal data among holding companies, subsidiaries, or affiliates under the common control of the same group as that of the data controller, or to a parent company or to any company belonging to the same group as that of the data controller, the mechanism to ensure that the receiver of the personal data complies with the provisions of the Law, these Regulations, and other applicable laws and regulations, may be the existence of internal rules to protect personal data whose observance is obligatory, provided that these comply with the requirements of the Law, these Regulations, and other applicable laws and regulations. Section III - International Transfers Specific Conditions Applicable to International Transfers Article 74. Without prejudice to the provisions of Article 37 of the Law, international transfers of personal data will be possible when the receiver of the personal data assumes the same obligations as those of the data controller transferring the personal data. Formalization of International Transfers Article 75. For such purposes, a data controller that transfers personal data may use contracts and other legal instruments which contain at least the same obligations as those to which the data controller transferring personal data is subject, as well as the conditions under which the data subject consented to the processing of his personal data. Opinion of the Institute Concerning Transfers Article 76. Data controllers, if considered necessary, may request the opinion of the Institute as to whether an international transfer that they are carrying out complies with the Law and these Regulations.	Ministry of the Economy, Regulations to the Federal Law on the Protection of Personal Data Held by Private Parties

Title	Types of Data Covered	Selected Rules in Mexico on Cross-Border Data Transfers or Data Localization	Sources
LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS Nueva Ley publicada en el Diario Oficial de la Federación el 26 de enero de 2017		Not excerpted or summarized due to lack of translation.	http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Moldova

Title	Types of Data Covered	Selected Rules in Republic of Moldova on Cross-Border Data Transfers or Data Localization	Sources
Law No. 133 of 8 July 2011 on Personal Data Protection	Personal	Not excerpted or summarized due to lack of translation.	http://ilo.ch/dyn/natlex/natlex4.detail?p_lang=en&p_isn=89948&p_count=100183&p_classification=01&p_classcount=13206

Title	Types of Data Covered	Selected Rules in Monaco on Cross-Border Data Transfers or Data Localization	Sources
Act n° 1.165 On the protection Of personal data (23 December 1993)	Personal	Excerpt (translated version) CHAPTER 3bis - ON THE TRANSFER OF PERSONAL DATA Article 20. - The transfer of personal data outside the Principality may only take place subject to the condition that the country or organisation that is to be the recipient of the transfer has an adequate level of protection. The adequate nature of the level of protection afforded by the third country must be appreciated in the light of all circumstances relating to the transfer of personal data, in particular the nature of the data, the purpose, the duration of processing operation(s) envisaged, the rule of law in force in the country in question, and the professional rules and security measures complied with in the said country. Without prejudice to the foregoing provisions, the Commission de Contrôle des Informations Nominatives shall make available to any interested party a list of countries with an adequate level of protection within the meaning of the previous paragraph. Article 20-1. - The transfer of personal data to a country or organisation that does not provide, within the meaning of the second paragraph of Article 20, an adequate level of protection, may nevertheless take place if the data subject has consented to the transfer or if the transfer is required: - to safeguard that person's life; - to safeguard public interests; - to ensure the compliance with legal obligations with regards to the recording, exercising or defence of legal rights; - for the consultation, under proper conditions, of a public register which, by virtue of legislative or regulatory provisions, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest; - as part of a contract between the data controller or representative and the data subject, or pre-contractual measures taken at the latter's request; - the conclusion or as part of a contract concluded or to be concluded in the interests of the data subject, between the data controller or representative and a third party. Without prejudice to the provisions of the previous paragraph, the Commission de Contrôle des Informations Nominatives may authorise, on the basis of a duly substantiated application, a transfer of personal data to a country or organisation that does not have an adequate level of protection within the meaning of the second paragraph of Article 20 if the data controller or their representative, as well as the recipient of data, offer sufficient guarantees to ensure compliance with the protection of the rights and freedoms described in Article 1. Such safeguards may in particular result from appropriate contractual clauses. The data controller must comply with the Commission's decision.	https://www.ccin.mc/images/documents/act-1165-on-the-protection-of-personal-data.pdf
RAPPORT D'ACTIVITÉ 2019 11th rapport public PUBLIÉ EN APPLICATION DE L'ARTICLE2-14 DE LA LOI N°1.165 RELATIVE À LA PROTECTION DESINFORMATI	Personal	Not excerpted or summarized due to lack of translation.	https://www.ccin.mc/fr/ccin/notre-actualite/197-11eme-rapport-public-2

Title	Types of Data Covered	Selected Rules in Monaco on Cross-Border Data Transfers or Data Localization	Sources
ONS NOMINATIVES			

Mongolia

Title	Types of Data Covered	Selected Rules in Mongolia on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	On 17 December 2021, the Parliament of Mongolia (the "**Parliament**") adopted the Law of Mongolia on Personal Data Protection (the "**Data Protection Law**") which will come into effect and full force from 1 May 2022. The Data Protection Law applies to matters related to personal privacy and relations in connection with the collecting, processing, using, and security of Personal Data (as defined below) of an individual, as well as the collection, processing and use of individual's Personal Data with the help of technology and software. The Data Protection Law regulates the handling of Personal Data and Sensitive Personal Data by Data Controller. Under the Data Protection Law, transfer of Personal Data to is prohibited unless otherwise approved under the relevant laws or permitted by the Data Owner.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=MN
Law on information transparency and right to information, 2011 (updated in 2015)	Personal	Not excerpted or summarized due to lack of translation.	https://www.iaac.mn/old/pdf/law_en/6_law_on_the_information_transparency_and_right_to_information.pdf

Montenegro

Title	Types of Data Covered	Selected Rules in Montenegro on Cross-Border Data Transfers or Data Localization	Sources
Law on Protection of Personal Data No. 79/2009, 70/2009, 44/2012, 22/2017	Personal	Excerpt IV TRANSFER OF PERSONAL DATA FROM MONTENEGRO Article 41 Personal data undergoing processing may be transferred from Montenegro to another country or given to an international organisation, which implements safeguards provided for by this law, with the prior consent of the supervisory authority. The adequacy of the measures of protection referred to in paragraph 1 of this Article shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to: 1) the nature of the data; 2) the purpose and duration of the proposed processing operation or operations; 3) the country of origin and country of final destination, 4) the rules of law in force in the third country in question and 5) the professional rules and security measures which are complied with in that country. A transfer of data with the purpose of entrusting specific processing activities within the meaning of Article 16 of this law may take place only with the consent of the supervisory authority, except in the case set out in Article 42 item 6 of this law. Article 42 The consent referred in Article 41, paragraph 1 of this Law shall not be mandatory where: 1) the transfer of personal data is provided for by a separate law or an international treaty binding on Montenegro; 2) the data subject has given his prior consent to the proposed transfer and has been informed of possible consequences of data transfer; 3) the transfer is required for the performance of a contract between a legal or natural person and the personal filing system data controller or the implementation of precontractual obligations; 4) the transfer is required in order to protect the life of the data subject or is in his interest; 5) the transfer is made from a register or records which according to laws or other regulations are available to the public; 6) the data are transferred to the Member States of the European Union and European Economic Area or countries which are included on the European Union list of countries with an adequate level of personal data protection; 7) the transfer is necessary on important public interest grounds, or for the establishment, exercise or defence of legal claims of the data subject; 8) the personal data filing system controller concludes a contract stipulating adequate contractual obligations accepted by the Member States of the European Union, with a personal data processor from the third country, and where 9) the transfer is necessary for the conclusion or performance of a contract between the personal data filing system controller and a legal or natural person concluded in the interest of the data subject.	https://www.afapdp.org/wp-content/uploads/2012/01/Mont%c3%a9n%c3%a9gro-Personal-Data-Protection-Law-79-08-and-70-09.pdf

Morocco

Title	Types of Data Covered	Selected Rules in Morocco on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Morocco's law governing privacy and data protection is Law No 09-08, dated February 18, 2009 relating to protection of individuals with regard to the processing of personal data and its implementation Decree n° 2-09-165 of May 21, 2009 (together the DP Law). Prior authorization from the National Commission is required before any transfer of personal data to a foreign state. Further, the person in charge of the processing operation can transfer personal data to a foreign state only if the said state ensures under its applicable legal framework an adequate level of protection for the privacy and fundamental rights and freedoms of individuals regarding the processing to which these data is or might be subject, unless: • The data subject has expressly consented to the transfer • The transfer and subsequent processing is required for: o Compliance with a legal obligation to which the concerned person or the person in charge of the processing are submitted o The execution of a contract to which the concerned person is party or in the performance of pre-contractual measures taken at the request of the latter o The protection of the vital interests of the relevant data subject, if that person is physically or legally unable to give its consent o Performance of a task of public interest or related to the exercise of public authority, vested in the person in charge of the processing or the third party to whom the data are communicated o Fulfillment of the legitimate interests pursued by the data controller or by the recipient, when not outweighed by the interests or fundamental rights and freedoms of the relevant data subject In practice, we notice that CNDP interprets the exception of legitimate interests of the data processor very restrictively. CNDP is in general more comfortable relying on the data subject's consent regarding any transfers to a foreign state.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=MA
Law No. 09-08/2009 on the protection of people toward data protection of a personal nature	Personal	Not excerpted due to lack of translation.	https://www.dgssi.gov.ma/sites/default/files/attached_files/loi_09-08protection_donnees_personnelles.pdf

Nepal

Title	Types of Data Covered	Selected Rules in Nepal on Cross-Border Data Transfers or Data Localization	Sources
The Privacy Act, 2075 (2018) Act Number 14 of the year 2075 (2018)	Personal	No provisions relating to international data transfer	https://www.lawcommission.gov.np/en/wp-content/uploads/2019/07/The-Privacy-Act-2075-2018.pdf

Namibia

Title	Types of Data Covered	Selected Rules in Namibia on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Namibia has not enacted comprehensive data privacy legislation. However, various sector-specific laws are in place to protect client information, including in the legal and banking sectors. Namibia recognizes the right to privacy as a fundamental human right under Article 13 of the Namibian Constitution. Accordingly, all persons have a right to privacy in their homes and communications. The right to privacy is limited as required by law and in the interest of protecting: • national security and public safety • the nation's economy • health and morals • against disorder and crime • the rights and freedoms of others The Namibian Government is currently drafting a Data Protection Policy that, although not yet public, is expected to: • protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to data processing • protect Namibian citizens from abuse of their personal data, and • harmonize Namibia's data protection policy and legal framework with regional and international standards to promote the free flow of personal data under conditions of assurance and trust There are no data transfer restrictions in place.	https://www.dlapiperdataprotection.com/index.html?t=law&c=NA

Netherlands

Title	Types of Data Covered	Selected Rules in Netherlands on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	See Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

New Zealand

Title	Types of Data Covered	Selected Rules in New Zealand on Cross-Border Data Transfers or Data Localization	Sources
Privacy Act 1993: repealed, on 1 December 2020, by section 216(1) of the Privacy Act 2020 (2020 No 31)	Personal	Excerpt **Part 11A** - Transfer of personal information outside New Zealand (Part 11A: inserted, on 8 September 2010, by section 8 of the Privacy (Cross-border Information) Amendment Act 2010 (2010 No 113)) **114A** - Interpretation In this Part, unless the context otherwise requires,— OECD Guidelines means the Organisation for Economic Co-operation and Development Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data State includes any State, territory, province, or other part of a country transfer prohibition notice means a notice given under section 114B prohibiting the transfer of personal information from New Zealand to another State. **114B** - Prohibition on transfer of personal information outside New Zealand (Section 114B: inserted, on 8 September 2010, by section 8 of the Privacy (Cross-border Information) Amendment Act 2010 (2010 No 113)). (1) The Commissioner may prohibit a transfer of personal information from New Zealand to another State if the Commissioner is satisfied, on reasonable grounds, that— (a) the information has been, or will be, received in New Zealand from another State and is likely to be transferred to a third State where it will not be subject to a law providing comparable safeguards to this Act; and (b) the transfer would be likely to lead to a contravention of the basic principles of national application set out in Part Two of the OECD Guidelines and set out in Schedule 5A. (2) In determining whether to prohibit a transfer of personal information, the Commissioner must also consider, in addition to the matters set out in subsection (1) and section 14, the following: (a) whether the transfer affects, or would be likely to affect, any individual; and (b) the general desirability of facilitating the free flow of information between New Zealand and other States; and (c) any existing or developing international guidelines relevant to transborder data flows, including (but not limited to)— (i) the OECD Guidelines: (ii) the European Union Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. (3) Subsection (1) does not apply if the transfer of the information, or the information itself, is— (a) required or authorised by or under any enactment; or (b) required by any convention or other instrument imposing international obligations on New Zealand. **114C** - Commissioner's power to obtain information (Section 114C: inserted, on 8 September 2010, by section 8 of the Privacy (Cross-border Information) Amendment Act 2010 (2010 No 113)). (1) To enable the Commissioner to determine whether to prohibit a transfer of personal information, the Commissioner may hear or obtain information from such persons as the Commissioner considers necessary, and for this purpose Part 9 applies as if the Commissioner were carrying out an inquiry under section 13(1)(m). (2) In exercising his or her powers under subsection (1), the Commissioner may regulate his or her procedure in such manner as the Commissioner thinks fit.	https://www.legislation.govt.nz/act/public/1993/0028/latest/whole.html#DLM3242823

Title	Types of Data Covered	Selected Rules in New Zealand on Cross-Border Data Transfers or Data Localization	Sources
		114D - Transfer prohibition notice (Section 114D: inserted, on 8 September 2010, by section 8 of the Privacy (Cross-border Information) Amendment Act 2010 (2010 No 113)) (1) A prohibition under section 114B(1) is to be effected by the service of a transfer prohibition notice on the agency proposing to transfer the personal information concerned. (2) A transfer prohibition notice must— (a) state the name of the agency to whom it relates; and (b) describe the personal information concerned; and (c) state that the transfer of the personal information concerned from New Zealand to a specified State is prohibited either— (i) absolutely; or (ii) until the agency has taken the steps stated in the notice to protect the interests of any individual or individuals affected by the transfer; and (d) state the time when the notice takes effect; and (e) state the ground for the prohibition; and (f) state that the agency on whom the notice is served may lodge an appeal against the notice to the Human Rights Review Tribunal, and the time within which the appeal must be lodged. (3) The time when the notice takes effect under subsection (2)(d) must not be before the end of the period within which an appeal against the notice can be lodged. (4) If an appeal is brought, the notice does not take effect pending the determination or withdrawal of the appeal. (5) If the Commissioner, by reason of special circumstances, considers that the prohibition should take effect as a matter of urgency in relation to all or any part of the notice,— (a) subsections (3) and (4) do not apply; and (b) the notice takes effect on the sixth working day after the date on which the notice is served; and (c) the notice must include— (i) a statement that the Commissioner considers that the prohibition must take effect as a matter of urgency; and (ii) a statement of the reasons why the Commissioner has reached that conclusion. **114E** - Commissioner may vary or cancel notice (Section 114E: inserted, on 8 September 2010, by section 8 of the Privacy (Cross-border Information) Amendment Act 2010 (2010 No 113)) (1) If, at any time, the Commissioner considers that all or any of the provisions of a transfer prohibition notice served on an agency need not be complied with in order to avoid a contravention of basic principles of privacy or data protection, the Commissioner may vary or cancel the transfer prohibition notice by serving notice to that effect on the agency concerned. (2) An agency on whom a transfer prohibition notice has been served may, at any time after the end of the period during which an appeal under section 114G(1)(a) can be lodged, apply in writing to the Commissioner for the notice to be varied or cancelled under subsection (1). (3) The Commissioner must, within 20 working days after the date on which an application under subsection (2) is received, notify the agency of— (a) his or her decision; and (b) his or her reasons, if the application is refused. (4) If the Commissioner exercises his or her discretion under subsection (1), the variation or cancellation of the transfer prohibition notice takes effect on the day after the date on which notice of the Commissioner's decision to vary or cancel the transfer prohibition notice is served. **114F** - Offence in relation to transfer prohibition notice (Section 114F: inserted, on 8 September 2010, by section 8 of the Privacy (Cross-border Information) Amendment Act 2010 (2010 No 113). Section 114F: amended, on 1 July 2013, by section 413 of the Criminal Procedure Act 2011 (2011 No 81))	

Title	Types of Data Covered	Selected Rules in New Zealand on Cross-Border Data Transfers or Data Localization	Sources
		Every person who, without reasonable excuse, fails or refuses to comply with a transfer prohibition notice commits an offence and is liable on conviction to a fine not exceeding $10,000. **114G -** Appeals against transfer prohibition notice (Section 114G: inserted, on 8 September 2010, by section 8 of the Privacy (Cross-border Information) Amendment Act 2010 (2010 No 113)) (1) An agency on whom a transfer prohibition notice is served may appeal to the Human Rights Review Tribunal— (a) against the whole or any part of the notice; or (b) if the notice contains a statement by the Commissioner in accordance with section 114D(5)(c), against the decision to include that statement in respect of all or any part of the notice; or (c) against the decision of the Commissioner to vary the notice in accordance with section 114E(1); or (d) against the refusal of an application under section 114E(2) to vary or cancel the notice. (2) An appeal under subsection (1) must be lodged,— (a) in the case of an appeal under subsection (1)(a) or (b), within 15 working days from the date on which the transfer prohibition notice was served on the agency concerned: (b) in the case of an appeal under subsection (1)(c) or (d), within 15 working days from the date on which notice of the decision or refusal was served on the agency concerned. (3) The Tribunal must allow an appeal or substitute any other decision or notice that could have been made or served by the Commissioner if it considers that— (a) the decision or notice against which the appeal is brought is not in accordance with the law; or (b) to the extent that the decision or notice involved an exercise of discretion by the Commissioner, the Commissioner ought to have exercised his or her discretion differently. (4) The Tribunal may review any determination of fact on which the decision or notice in question was based. (5) On any appeal under subsection (1)(b), the Tribunal may— (a) direct— (i) that the notice in question must have effect as if it did not contain the statement that is mentioned in the notice; or (ii) that the inclusion of the statement must not have effect in relation to any part of the notice; and (b) make any modifications required to give effect to that direction. **114H** - Application of Human Rights Act 1993 (Section 114H: inserted, on 8 September 2010, by section 8 of the Privacy (Cross-border Information) Amendment Act 2010 (2010 No 113)) Section 87 and Part 4 of the Human Rights Act 1993 apply, with all necessary modifications (if any), in relation to proceedings under section 114G as if they were proceedings under that Act.	

Nicaragua

Title	Types of Data Covered	Selected Rules in Nicaragua on Cross-Border Data Transfers or Data Localization	Sources
Ley No. 787 Ley de Protección de Datos Personales (in Spanish)	Personal	Pdf link not found	http://www.pgr.gob.ni/PDF/Constitucional/ley%20787.pdf

Niger

Title	Types of Data Covered	Selected Rules in Niger on Cross-Border Data Transfers or Data Localization	Sources
Loi n°2017-28 du 03 Mai 2017 relative à la protection des données à caractère personnel, révisé en 2019 (In French)	Personal	Article 24: Le responsable d'un traitement ne peut etre autorise a transferer des donnees a caractere personnel vers un pays tiers que si cet Etat assure un niveau de protection superieur ou equivalent de la vie prive, des libertes et droits fondamentaux des personnes a l'egard du traitement dent ces donees font ou peuvent faire l'objet. Avant tout transfer effectif des donnees a caractere personnel vers ce pays tiers, le responsable du traitement doit prealablement obtenir l'autorisation de l'Autorite de protection au regard de leur finalite. *Machine translation:* *The controller may be authorised to transfer personal data to a third country only if that State ensures a higher or equivalent level of protection of the privacy, fundamental rights and freedoms of persons with regard to the processing to which such data are or may be subject.* *Before any effective transfer of personal data to this third country, the controller must first obtain the authorization of the Protection Authority with regard to their purpose.*	https://www.afapdp.org/wp-content/uploads/2017/02/Loi-n%c2%b02017-28-du-03-mai-2017.pdf

Nigeria

Title	Types of Data Covered	Selected Rules in Nigeria on Cross-Border Data Transfers or Data Localization	Sources
Summary		In 2019, pursuant to its powers under the NITDA Act of 2007, the National Information Technology Development Agency (NITDA) issued the Nigeria Data protection Regulation (NDPR). It is the principal regulation for data protection in Nigeria. In 2020, NITDA also issued an Implementation Framework in respect of the NDPR and also Guidelines for the Management of Personal Data by Public Institutions in Nigeria to regulate personal data processing within public institutions The NDPR includes provisions on Personal Data transfers to foreign countries and international organizations, provided such transfers are intended for processing purposes. The Honorable Attorney General of the Federation (HAGF) is responsible for supervising such Personal Data transfers. Personal Data transfers are permitted where NDPB determines that a foreign country, territory or specific sector(s) within a foreign country or international organization provide adequate levels of Personal Data protection. The determination is based on the HAGF's consideration of the foreign country's legal system, rule of law, respect for human rights and fundamental freedoms, as well as relevant general and sector-specific legislation in public security, defense, national security and criminal law. Personal Data transfers may take place without NDPB or HAGF authorization if: • Data Subject expressly consents to the proposed transfer after being informed of associated risks in the absence of an adequacy determination, the lack of appropriate safeguards, and that there are no alternatives; • Transfer is necessary for the performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request; • Transfer is necessary for the performance of a contract in the interests of the Data Subject between the Controller and another natural or legal person; • Transfer is necessary for important reasons of public interest; • Transfer is necessary for the establishment, exercise or defense of legal claims; • Transfer is necessary to protect the vital interests of the Data Subject or of other persons, where the data subject is physically or legally incapable of giving consent; or • Where Personal Data is transferred to a foreign country or to an international organization, the Data Subject shall have the right to be informed of the appropriate safeguards for data protection in the foreign country. In October 2022, a draft Federal Data Protection Bill was issued to establish the Nigerian Data Protection Commission, regulate data retention, international data transfers and data breaches.	Transfer in Nigeria - DLA Piper Global Data Protection Laws of the World (dlapiperdataprotection.com)
Data Protection Bill, 2022	Personal	**Data Protection Bill, 2022** PART IX—CROSS-BORDER TRANSFERS OF PERSONAL DATA 43. — (1) A data controller or data processor shall not transfer personal data from Nigeria to another country unless— (a) the recipient of the personal data is subject to a law, binding corporate rules, contractual clauses, code of conduct or certification mechanism that affords an adequate level of protection with respect to the personal data in accordance with section 44; or (b) one of the conditions set forth in section 45 applies. (2) A data controller or data processor shall record the basis for transfer of personal data to another country under subsection (1) and the adequacy of protection under section 44, if applicable. (3) The Commission may make rules requiring data controllers and data processors to notify it of the measures in place under subsection (1) and to explain their adequacy in terms of section 44, if applicable. (4) The Commission may designate categories of personal data that are subject to additional specified restrictions on transfer to another country based on the nature of such personal data and risks to data subjects.	Nigeria_Data_Protection_Bill.pdf (ndpb.gov.ng)

Title	Types of Data Covered	Selected Rules in Nigeria on Cross-Border Data Transfers or Data Localization	Sources
		44. — (1) A level of protection is adequate for the purposes of section 43(1)(a) if it upholds principles that are substantially similar to the conditions for processing of the personal data provided for in this Act, including in relation to the onward transfer of personal data to other countries. (2) The adequacy of protection referred to in subsection (1) shall be assessed taking into account: (a) the availability of enforceable data subject rights, the ability of data subjects to enforce their rights through administrative or judicial redress, and the rule of law generally; (b) the existence of any legally binding instrument between the Commission and a relevant public Commission in the recipient country addressing elements of adequate protection referred to in subsection (1); (c) the access of a public authority to personal data; (d) the existence of an effective data protection law; (e) the existence and functioning of an independent, competent data protection or similar supervisory authority with adequate enforcement powers; and (f) international commitments and conventions binding on the relevant country and its membership of any multilateral or regional organisations. (3) The Commission shall issue a guideline as to the assessment of adequacy and the factors set forth under subsection (2). (4) The Commission may from time to time designate any country, region or specified sector within a country, or standard contractual clauses as affording or as not affording an adequate level of protection under subsection (1). (5) The Commission may approve binding corporate rules, codes of conduct or certification mechanisms proposed to it by a data controller, where the Commission determines that the aforesaid meets the adequacy requirements of subsection (1). (6) The absence of a determination by the Commission under subsection (4) or (5) with respect to a country, territory, sector, binding corporate rule, contractual clause, code of conduct or certification mechanism shall not imply the adequacy of the protections afforded by it. (7) The Commission may make a determination under subsection (4) based on adequacy decisions made by competent data protection authorities of other jurisdictions Adequacy of protection where such decisions have taken into account factors similar to those listed in subsection (2). 45. In the absence of adequacy of protection under section 44, a data controller or data processor shall only transfer personal data from Nigeria to another country if— (a) the data subject has given and not withdrawn consent to such transfer after having been informed of the possible risks of such transfers for the data subject due to the absence of adequate protections; (b) the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party; or (d) the transfer is for the benefit of the data subject and— (i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and (ii) if it were reasonably practicable to obtain such consent, the data subject would likely give it.	
NIGERIA DATA PROTECTION REGULATION 2019	Personal	Excerpt **2.11 TRANSFER TO A FOREIGN COUNTRY** Any transfer of Personal Data which is undergoing processing or is intended for processing after transfer to a foreign country or to an international organisation shall take place subject to the other provisions of this Regulation and the supervision of the Honourable Attorney General of the Federation (HAGF). Accordingly: a) a transfer of Personal Data to a foreign country or an international organization may take place where the Agency has decided that the foreign country, territory or one or more specified sectors within that foreign country, or the international organization in question ensures an adequate level of protection; b) the HAGF shall take into consideration the legal system of the foreign country particularly in the areas of rule of law, respect for human rights and fundamental freedom, relevant legislation, both general and sectoral, including public security, defence, national security and criminal law and the access of public authorities to Personal Data;	https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf

Title	Types of Data Covered	Selected Rules in Nigeria on Cross-Border Data Transfers or Data Localization	Sources
		c) implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of Personal Data to another foreign country or international organization which are complied with in that country or international organization, caselaw, as well as effective and enforceable Data Subject rights and effective administrative and judicial redress for the Data Subjects whose Personal Data are being transferred; d) the existence and effective functioning of one or more independent supervisory authorities in the foreign country or to which an international organization is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the Data Subjects in exercising their rights and for cooperation with the relevant authorities in Nigeria; and e) the international commitments of the foreign country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, particularly in relation to the protection of Personal Data. **2.12 EXCEPTIONS IN RESPECT OF TRANSFER TO A FOREIGN COUNTRY** In the absence of any decision by The Agency or HAGF as to the adequacy of safeguards in a foreign country, a transfer or a set of transfers of Personal Data to a foreign country or an international organisation shall take place only on one of the following conditions: a) that the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers; b) the transfer is necessary for the performance of a contract between the Data Subject and the Controller or the implementation of precontractual measures taken at the Data Subject's request; c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person; d) the transfer is necessary for important reasons of public interest; e) the transfer is necessary for the establishment, exercise or defence of legal claims; and f) the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent; Provided, in all circumstances, that the Data Subject has been manifestly made to understand through clear warnings of the specific principle(s) of data protection that are likely to be violated in the event of transfer to a third country, this proviso shall not apply to any instance where the Data Subject is answerable in duly established legal action for any civil or criminal claim in a third country.	
Central Bank of Nigeria, Guidelines on Point of Sale Card Acceptance Services (2011)	Financial	Summary: “Guideline 4.4.8 requires entities engaging in point of sale (POS) card acceptance services in Nigeria to use a local network switch (which connects devices and processes information to and from connected devices) for all domestic POS and ATM transactions. Domestic transactions cannot be routed outside Nigeria for switching between Nigerian issuers and acquirers.”	Thompson Reuters, Data Localization Laws - Nigeria
National Information Technology Development Agency, Mandatory Guidelines for	Various	Summary: • “Guideline 9.1 requires all Indigenous Original Equipment Manufacturers (companies that produce functional computer devices from component parts bought from other organizations) to assemble all hardware in Nigeria and maintain fully staffed facilities for that purpose. • Guideline 11.1(4) requires all telecommunications companies to host all subscriber and consumer data in Nigeria. • Guideline 12.1(4) requires all network service companies to host all subscriber and consumer data in Nigeria. • Guideline 12.2(1) requires all ministries, departments, and agencies of Nigeria’s federal government (MDAs) to host their websites locally and under a registered.gov.ng domain. • Guideline 13.1(2) requires all data and information management companies to host all sovereign data in Nigeria.	NITDA, Guidelines for Nigerian Content Development in Information and Communication Technology

Title	Types of Data Covered	Selected Rules in Nigeria on Cross-Border Data Transfers or Data Localization	Sources
Nigerian Content Development in Information and Communication Technology (ICT) (2019)		Guideline 13.2(3) requires MDAs to host all sovereign data locally on servers within Nigeria".	Thompson Reuters, Data Localization Laws - Nigeria

Norway

Title	Types of Data Covered	Selected Rules in Norway on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	See Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Oman

Title	Types of Data Covered	Selected Rules in Oman on Cross-Border Data Transfers or Data Localization	Sources
Royal Decree No. 6 of 2022 promulgating the law on the protection of personal data dated 9 February 2022 ('the Law') (only available in Arabic)	Personal	Not excerpted or summarized due to lack of translation.	https://decree.om/2022/rd20220006/

Pakistan

Title	Types of Data Covered	Selected Rules in Pakistan on Cross-Border Data Transfers or Data Localization	Sources
Summary	Various	Pakistan currently has not enacted data protection legislation per se similar to data protection legislation enacted in other countries of the world, however the Prevention of Electronic Crimes Act, 2016 ("PECA 2016") at present serves the same purpose to a certain extent. Moreover, a consultation draft of the Personal Data Protection Bill 2020 ("PDPB") has been introduced by the Ministry of Information Technology and Telecommunications with a view to having the same being promulgated into law after public consultation, approval from both Houses of Parliament and receipt of assent from the President of Pakistan. Section 16 prohibits the transmission of identity information of a person without consent. In addition, Pakistan prohibits data transfers to any country that it does not recognize, including: Israel, Taiwan, Somaliland, Nagorno, Karabakh, Transnistria, Abkhazia, Northern Cyprus, Sahrawi Arab Democratic Republic, South Ossetia and Armenia. This list may change from time to time. Additionally, data transfers to India must be justifiable by the transferor. Data collated by banks, insurance firms, hospitals, defense establishments and other 'sensitive' institutions may not be transferred to any individual or body without authorization from the relevant regulator on a confidential basis. Such data is further regulated by contractual terms. In certain cases, data may not be transferred without authorization from the data subject. Similarly, the PDPB, which is yet to be promulgated, proposes prohibiting the transfer of personal data to unauthorized persons or systems. Where the transfer of personal data pertains to a transfer to a territory outside of Pakistan, the PDPB would require the territory where personal data is to be transferred to offer an equivalent degree of personal data protection as that provided for in Pakistan, provided that such data transfer is done in accordance with a framework for the transfer of personal data outside of Pakistan as devised by the Authority.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=PK
PERSONAL DATA PROTECTION BILL 2021 CONSULTATION DRAFT: V.25.08.2021	Personal	Excerpt **14 CROSS BORDER TRANSFER OF PERSONAL DATA** 14.1 If personal data is required to be transferred to any system located beyond territories of Pakistan or system that is not under the direct control of government of Pakistan or entity/entities of Pakistan, it shall be ensured that the country where the data is being transferred offers personal data protection legal regime at least equivalent to the protection provided under this Act and the data so transferred shall be processed in accordance with this Act and, where applicable, the consent given by the data subject. 14.2 Critical Personal Data shall only be processed in a server or data centre located in Pakistan. **15 FRAMEWORK ON CONDITIONS FOR CROSS-BORDER TRANSFER OF PERSONAL DATA** 15.1 Personal data other than those categorize as critical personal data may be transferred outside the territory of Pakistan under a framework (on conditions) to be devised by the Commission. 15.2 The Commission shall also devise a mechanism for keeping some components of the of sensitive personal data in Pakistan to which this act applies, provided that related to public order or national security.	https://moitt.gov.pk/SiteImage/Misc/files/25821%20DPA%20Bill%20Consultation%20Draft_docx.pdf
PERSONAL DATA PROTECTION BILL, 2020 CONSULTATION DRAFT (April 2020 draft)	Personal	**14 CROSS BORDER TRANSFER OF PERSONAL DATA** Provided that if personal data is required to be transferred to any system located beyond territories of Pakistan or system that is not under the direct control of any of the governments in Pakistan, it shall be ensured that the country where the data is being transferred offers personal data protection at least equivalent to the protection provided under this Act and the data so transferred shall be processed in accordance with this Act and, where applicable, the consent given by the data subject.	Ministry of Information Technology & Telecommunication, Personal Data Protection Bill

		14.1 Critical personal data shall only be processed in a server or data centre located in Pakistan. 14.2 Notwithstanding anything contained in sub-section (1), the Federal Government may notify certain categories of personal data as exempt from the requirement under sub-section (1) on the grounds of necessity or strategic interests of the State. 14.3 Nothing contained in sub-section (3) shall apply to sensitive personal data. **15 FRAMEWORK ON CONDITIONS FOR CROSS-BORDER TRANSFER OF PERSONAL DATA. —** 15.1 Personal data other than those categorize as critical personal data may be transferred outside the territory of Pakistan under a framework (on conditions) to be devised by the Authority. 15.2 The Authority shall also devise a mechanism for keeping a copy of personal data in Pakistan to which this act applies.	2020, Consultation Draft v. 09.04.2020 US State Dep't, Pakistan Investment Climate Digital Rights Foundation, Civil Society Submission on Personal Data Protection Bill

Panama

Title	Types of Data Covered	Selected Rules in Panama on Cross-Border Data Transfers or Data Localization	Sources
Ley 81, Protección de datos personales, 2019	Personal	Not excerpted or summarized due to lack of translation.	https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf

Paraguay

Title	Types of Data Covered	Selected Rules in Paraguay on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Law No. 6534/2020 “of protection of personal credit data” (“Personal Credit Data Protection Law” or “Law”). The previous data protection regulatory regime lead by Law No. 1682/2001 “which regulates the use of private information” as amended by laws No. 1969/2002 and 5543/2015 is no longer in force and was replaced in full by the Personal Credit Data Protection Law (Art. 30 of the Law). The Personal Credit Data Protection Law establishes that international transfers of personal data to a recipient that is in a third country (as defined under the Law), or to an international organization where the guarantees, requirements and/or exceptions established in the Law are not met, is a violation of applicable data protection law and, thus, can be subject to sanctions (Art. 21.x. of the Law). Under current legislation, there are no other specific provisions that regulate the transfer of private information. However, the transfer of private information is considered as a form of data processing, so the same rules than for collection and processing personal data applies (Art. 3.e. of the Law – definition treatment of data).	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=PY
Ley 1682/2001 Reglamenta la Informacion de Caracter Privado (in Spanish)		Not excerpted or summarized due to lack of translation.	http://www.oas.org/es/sla/ddi/docs/PA6%20Ley%20N%201682%20de%202001.pdf
Ley Nº 1969/2002 “Que modifica, amplía y deroga varios artículos de la Ley Nº 1682/2001”		Not excerpted or summarized due to lack of translation.	http://digesto.senado.gov.py/ups/leyes/10389.pdf
Ley Nº 5543/2015 “Que modifica parcialmente la Ley Nº 1969/2002”		Not excerpted or summarized due to lack of translation.	https://www.bacn.gov.py/archivos/4524/20160224131953.pdf
Ley Nº 5830/2017 “Que prohíbe la publicidad no autorizada por los usuarios titulares de telefonía móvil”		Not excerpted or summarized due to lack of translation.	https://drive.google.com/file/d/1Sa1-pI1tCPffeTVqNCiVb-tLyvjHBzlx/view
Decreto Nº 8000/2017 “Por el cual se reglamenta la Ley 5830/2017 Que		Not excerpted or summarized due to lack of translation.	https://drive.google.com/file/d/1YJGCA1i7W5Ok_t_JlNkSXw8ae__zdQG-/view

Title	Types of Data Covered	Selected Rules in Paraguay on Cross-Border Data Transfers or Data Localization	Sources
prohíbe la publicidad no autorizada por los usuarios titulares de telefonía móvil”			
Resolución Nº 80/2018 “Por la cual se aprueba la normativa reglamentaria de la Ley Nº 5830 Que prohíbe Que prohíbe la publicidad no autorizada por los usuarios titulares de telefonía móvil”		Not excerpted or summarized due to lack of translation.	https://drive.google.com/file/d/1Uzc78s9ZSTOGPwmcn1kRVHTp9U_EwKle/view

Peru

Title	Types of Data Covered	Selected Rules in Peru on Cross-Border Data Transfers or Data Localization	Sources

Ley N° 29733 - Ley de Protección de Datos Personales (in Spanish)		Article 2 of the Political Constitution of Peru sets forth certain fundamental rights that every person has, including a right to privacy regarding information that affects personal and family privacy. The Personal Data Protection Law N° 29733 (PDPL) was enacted in June 2011. In March 2013, the Supreme Decree N° 003-2013-JUS-Regulation of the PDLP (Regulation) was published in order to develop, clarify and expand on the requirements of the PDPL and set forth specific rules, terms and provisions regarding data protection.
		
		Further, the law regulating private risk centers and the protection of the owner of the information is Law Nº 27489, enacted in 2001 and later amended several times. This law establishes the applicable provisions for activities related to risk centers and companies that handle:
		
		• Information posing higher risks to individuals (*eg*, related to financial, commercial, tax, employment or insurance obligations or background of a natural or legal person that allows evaluating its economic solvency), and
		• Sensitive personal data (according to the PDPL)
		
		Where personal data is transferred to another entity, recipients must be required to handle such personal data in accordance with the provisions of the PDPL and its Regulation. Generally, data subject consent is required.
		
		In the case of cross-border transfers, the transferring entity may not transfer personal data to a country that does not afford adequate protection levels (protections that are equivalent to those afforded by the PDPL or similar international standards). If the receiving country does not meet these standards, the sender must ensure that the receiver in the foreign country is contractually obligated to provide 'adequate protection levels' to the personal data, such as via a written agreement that requires that the personal data will be protected in accordance with the requirements of the PDPL, or under one of the following circumstances:
		
		• In accordance with international treaties in which Peru is a party
		• For purposes of international judicial cooperation or international cooperation among intelligence agencies to combat
		  o Terrorism
		  o Drug trafficking
		  o Money laundry
		  o Corruption
		  o Human trafficking, and
		  o Other forms of organized crime
		• When necessary for a contractual relationship with the data subject, or for a scientific or professional relationship
		• Bank or stock transfers concerning transactions in accordance with the applicable law
		• The transfer is performed to protect, prevent, diagnose or medically or surgically treat the data subject, or to perform studies of epidemiology or the like, provided a data dissociation procedure has been applied
		• The owner of the personal data has given its prior, informed, express and unequivocal consent to the transfer to the inadequate jurisdiction
		• Other exempt purposes established by the Regulations
			https://doc.contraloria.gob.pe/documentos/Cuadro_Ley_Proteccion_Datos_Personales.pdf
			
			https://www.dlapiperdataprotection.com/index.html?t=transfer&c=PE

		For both domestic and cross-border transfers, the recipient must assume the same obligations as the transferor of the personal data. The transfer must be formalized, such as by binding written contract, and capable of demonstrating that the holder of the database or the data controller communicated to the recipients the conditions in which the data subject consented to their processing.	

Philippines

Title	Types of Data Covered	Selected Rules in Philippines on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The Data Privacy Act of 2012 ("**Act**" or "**DPA**") or Republic Act No. 10173, which took effect on 8 September 2012, is the governing law on data privacy matters in the Philippines. The transfer of Personal Information is permitted without any restrictions or prerequisites, but the personal information controller remains responsible for Personal Information under its control or custody that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.	https://www.dlapiperdataprotection.com/index.html?t=law&c=PH
Data Privacy Act of 2012 (REPUBLIC ACT NO. 10173)	Personal	Excerpt **CHAPTER I – GENERAL PROVISIONS** **Section 6**. Extraterritorial Application. – This Act applies to an act done or practice engaged in and outside of the Philippines by an entity if: (a) The act, practice or processing relates to personal information about a Philippine citizen or a resident; (b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following: (1) A contract is entered in the Philippines; (2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and (3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and (c) The entity has other links in the Philippines such as, but not limited to: (1) The entity carries on business in the Philippines; and (2) The personal information was collected or held by an entity in the Philippines. **CHAPTER VI - ACCOUNTABILITY FOR TRANSFER OF PERSONAL INFORMATION** **Section 21.** Principle of Accountability. – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation. (a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party. (b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.	https://lawphil.net/statutes/repacts/ra2012/ra_10173_2012.html

Poland

Title	Types of Data Covered	Selected Rules in Poland on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	See Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Portugal

Title	Types of Data Covered	Selected Rules in Portugal on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	See Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Qatar

Title	Types of Data Covered	Selected Rules in Qatar on Cross-Border Data Transfers or Data Localization	Sources
Law No. 13 of 2016 Concerning Privacy and Protection of Personal Data	Personal	Not excerpted or summarized due to lack of translation.	https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/105417/128915/F-1244585259/ClarificationsNoteDetails%20(4).pdf

Romania

Title	Types of Data Covered	Selected Rules in Romania on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	See Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Rwanda

Title	Types of Data Covered	Selected Rules in Rwanda on Cross-Border Data Transfers or Data Localization	Sources
Rwanda Draft Data Protection Law 2020	Personal	Excerpt **Article 52**: Remote access Any data controller and/or data processor shall not remotely access the data from another country unless authorized by the Authority in charge of data protection and privacy **Article 54**: Transfer or sharing of personal data outside Rwanda A data controller or data processor may transfer or share personal data to another country where: (a) he/she or it has the authorization granted by the Authority in charge of data protection and privacy after providing proof of appropriate safeguards with respect to the protection of the personal data; and (b) the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer owing to the absence of appropriate safeguards; (c) the transfer is necessary: (i) for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person; (iii) for reasons of public interest as provided by law; (iv) for the establishment, exercise or defense of a legal claim; or (v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or (vi) for the purpose of compelling legitimate interests pursued by the controller or the processor which are not overridden by the interests, rights and freedoms of the data subjects involved and where: (A) the transfer is not repetitive and concerns a limited number of data subjects; and (B) the controller or processor has assessed all the circumstances surrounding the data transfer operation and has, based on such assessment, provided to the Authority proof of appropriate safeguards with respect to the protection of the personal data; or (d) the transfer is made from a register which, according to law, is intended to provide information to the public and which is open for consultation by the public or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down by law for consultation are fulfilled in the particular case. A transfer pursuant to paragraph (1)(d) shall not involve the entirety of the personal data or entire categories of the personal data contained in the register and, where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or in case they are to be the recipients. Paragraph (1)(a) and (c)(i), (ii) and (vi) shall not apply to activities carried out by a public entity in the exercise of its functions. The Authority in charge of data protection and privacy may request a person who transfers data to another country to demonstrate the effectiveness of the safeguards or the existence of compelling legitimate interests and may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as it may determine.	https://www.dataguidance.com/sites/default/files/30802b_965abe73ea2e48899a28a4aefe2d3705.pdf

Saint Kitts and Nevis

Title	Types of Data Covered	Selected Rules in Saint Kitts and Nevis on Cross-Border Data Transfers or Data Localization	Sources
Data Protection Act 2018	Personal	No provision relating to international data transfer	https://www.dataguidance.com/sites/default/files/data_protection_act_5_of_2018.pdf

Saint Lucia

Title	Types of Data Covered	Selected Rules in Saint Lucia on Cross-Border Data Transfers or Data Localization	Sources
Data Protection (Amendment) Act, 2015 (No. 2 of 2015)	Personal	No provision relating to international data transfer	Data Protection (Amendment) Act.pmd (slugovprintery.com)
Data Protection Act, 2011	Personal	Excerpt **Transfer of personal data** **45.—(**1) Subject to subsection (2), a data controller shall not transfer personal data to a country or territory outside Saint Lucia unless – (a) the country or territory to which the personal data is being transferred has comparable safeguards to those in Saint Lucia for the protection of the rights and freedom of the data subject in relation to the processing of personal data; and (b) the Commissioner has authorized the data controller to transfer the personal data to the country or territory outside Saint Lucia. (2) Subsection (1)(a) does not apply if — (a) the data subject has given his or her consent to the transfer; (b) the transfer is necessary – (i) for the performance of a contract between the data subject and the data controller, or for the taking of steps at the request of the data subject with a view to entering into a contract with the data controller; (ii) for the conclusion of a contract between the data controller and a person, other than the data subject, which is entered at the request of the data subject, or is in the interest of the data subject for the performance of such a contract; or (iii) to safeguard national security or where section 56 applies; (c) the matter concerns public security; or (d) the transfer is made on such terms as may be approved by the Commissioner as ensuring the adequate safeguards for the protection of the rights of the data subject.	https://www.dataguidance.com/sites/default/files/act_11_of_2011.pdf

Saint Vincent and the Grenadines

Title	Types of Data Covered	Selected Rules in Saint Vincent and the Grenadines on Cross-Border Data Transfers or Data Localization	Sources
Data Protection Bill (Fourth Draft 6 October 2011)	Personal	No provision relating to international data transfer	https://www.oecs.org/en/our-work/knowledge/library/projects/egrip/data-protection-act

San Marino

Title	Types of Data Covered	Selected Rules in San Marino on Cross-Border Data Transfers or Data Localization	Sources
Law regulating the Computerized Collection of Personal Data 1983	Personal	Not excerpted or summarized due to lack of translation.	https://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/scheda17014317.html

Sao Tome and Principe

Title	Types of Data Covered	Selected Rules in Sao Tome and Principe on Cross-Border Data Transfers or Data Localization	Sources
Data Protection Act, 2016	Personal	Not excerpted or summarized due to lack of translation.	https://www2.camara.leg.br/saotomeeprincipe/diarios-da-an/x-legislatura/ii-serie/3.a-sessao-legislativa/DAN01-IIS.pdf/view

Title	Types of Data Covered	Selected Rules in Saudi Arabia on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	Under the PDPIR, Data Controllers may only store and process Personal Data outside KSA after obtaining written approval from the relevant "Regulatory Authority" and the Regulatory Authority must coordinate with the NDMO. "Regulatory Authority" is defined as *"Any independent governmental or public entity assuming regulatory duties and responsibilities for a specific sector in KSA under a legal instrument."* In the event Data Controllers are not subject to specific Regulatory Authorities, then the NDMO will exercise the roles and functions of such authorities. Data Controllers must also obtain NDMO's approval, having coordinated with the Regulatory Authority, prior to sharing Personal Data with other entities outside of KSA. Under the PDPL, data transfers out of KSA are even more tightly controlled than under the PDPIR. Personal Data transfers outside of KSA are prohibited except in the following circumstances: • extreme necessity to preserve the life of a Data Subject outside of KSA or the Data Subject's "vital interests"; • to prevent, examine or treat a disease; • if the transfer is in implementation of an obligation under which the KSA is a party; • to serve the interests of KSA; or • other purposes as determined by the Executive Regulations (yet to be issued). However, the above is still predicated upon complying with the following conditions: • the transfer or disclosure does not prejudice national security or the vital interests of KSA; • there are sufficient guarantees for preserving the confidentiality of the Personal Data to be transferred or disclosed, so that the standards are not less than the standards in the PDPL and the Executive Regulations; • the transfer or disclosure must be limited to the minimum Personal Data needed; and • the competent authority approves the transfer or disclosure, as determined by the Executive Regulations. However, the competent authority may exempt the Data Controller, on a case-by-case basis, from being bound by these conditions if: • the transfer does not prejudice national security or the vital interests of KSA; • if the competent authority, jointly or severally with other parties, sees that the Personal Data will have an acceptable level of protection outside of KSA; and • the Personal Data is not Sensitive Data. Note also that the relevant definitions for "processing" under both the PDPIR and PDPL include, amongst other things, transfer of Personal Data, and so the consent requirements relating to processing are also relevant / applicable. In addition, in certain contexts or sectors, specific approvals may be required - for example, in a banking context, approval from the Saudi Central Bank.	

Title	Types of Data Covered	Selected Rules in Saudi Arabia on Cross-Border Data Transfers or Data Localization	Sources
Personal Data Protection Law (November 2022) Issued by Royal Decree No. (M/19) dated 9/2/1443 AH	Personal	**Draft Personal Data Protection Law** Article 28 1- Controller may transfer Personal Data outside the Kingdom or disclose Personal Data to an entity outside the Kingdom in accordance with the following: a. If the country to which the Personal Data is to be transferred has regulations that ensure appropriate protection of Personal Data and protection of the rights of Personal Data Subjects, and has a supervisory entity that imposes appropriate procedures and measures on Controllers to protect Personal Data, so that the standards of Personal Data protection in that country are not less than the standards provided for under this Law and the Regulations. b. The Competent Authority adopts evaluation criteria for the requirements set out in paragraph (1.a) of this Article. 2- Notwithstanding paragraph 1 of this Article, in the following cases, Controller may transfer Personal Data to outside the Kingdom or disclose Personal Data to an entity outside the Kingdom in a manner other than as stated in paragraph (1.b) of this Article: a. If this is for preserving the public interest, public health, public safety, or protecting the life or health of a specific individual or individuals. b. If the transfer is relating to performing an obligation under an international agreement to which the Kingdom is a party. c. If this is done in performance of an obligation of the Personal Data Subject, in accordance with the applicable provisions set out in the Regulations. 3- When transferring Personal Data outside the Kingdom or disclosing Personal Data to an entity outside the Kingdom, the Controller shall observe the following: a. Such transfer shall not adversely affect the national security or vital interests of the Kingdom. b. The Transfer or Disclosure of Personal Data shall be limited to the minimum amount of Personal Data required. Article 29 1- Without prejudice to the provisions of this Law and the powers of the Saudi Central Bank pursuant to applicable legal provisions, the Competent Authority shall be the entity in charge of overseeing the implementation of this Law and the Regulations. 2- The Regulations shall identify the cases where the Controller shall appoint one or more persons as Personal Data protection officer(s), and shall set the responsibilities of any such person in accordance with the provisions of this Law. 3- The Controller shall cooperate with the Competent Authority in performing its duty to supervise the implementation of the provisions of this Law and the Regulations, and shall take such steps as necessary in connection with the related matters referred to the Controller by the Competent Authority. The Competent Authority may request documents and information from the Controller to ensure its compliance with this Law and the Regulations. 4- The Competent Authority may, at its sole discretion, authorize other entities to perform part of its responsibilities in connection with overseeing the implementation of the provisions of this Law and the Regulations. Article 30 1- Without prejudice to the provisions of Article 18 of this Law, the Controller shall keep records, for such a period as required under the Regulations, of the Personal Data Processing activities, based on the nature of the activity done by the Controller, so that such records are available whenever requested by the Competent Authority. The records shall contain the following information at a minimum: a. Contact details of the Controller. b. The purpose of the Processing. c. Description of the categories of Personal Data Subjects. d. Any other entity to which Personal Data has been or will be disclosed. e. Whether the Personal Data has been or will be transferred outside the Kingdom or disclosed to an entity outside the Kingdom. f. The expected period for which Personal Data shall be retained. 2- Controller shall keep records of the operations performed on Personal Data and shall set rules to restrict access to Personal Data. The Regulations shall set out the rules and procedures concerning those records. Article 31	https://istitlaa.ncc.gov.sa/en/Transportation/NDMO/PDPL22/Pages/default.aspx#!

Title	Types of Data Covered	Selected Rules in Saudi Arabia on Cross-Border Data Transfers or Data Localization	Sources
		In order to perform its obligations and supervise the implementation of this Law and the Regulations, the Competent Authority may issue decisions, instructions and circulars to enable the Competent Authority to monitor the Controllers' compliance with this Law and the Regulations. The Competent Authority shall have the following powers in particular: 1- Monitor compliance with this Law and the Regulations. 2- Issue guidelines, instructions and decisions relating to the enforcement of this Law and the Regulations, including decisions of precautionary measures and remedial actions to rectify any violation of this Law. 3- Seek assistance from other competent authorities to supervise the implementation of this Law and the Regulations. 4- Cooperate with its international counterparts entities in the cases that require supervising the implementation of this Law, without prejudice to the Kingdom's obligations under any international agreements, and in a manner that is not adverse to the Kingdom's international relations. 5- Take the necessary procedures to establish the violations of this Law, including carrying out detection and inspection activities. 6- Identify suitable tools and mechanisms to monitor the compliance of Controllers, including creating a national record for Controllers and providing services related to the protection of Personal Data. The Competent Authority may collect fees for the services it provides, in coordination with Ministry of Finance and the Non-Oil Revenues Development Center. 7- Identify suitable tools and mechanisms to monitor the compliance of the entities outside the Kingdom that process Personal Data of individuals residing in the Kingdom, and identify suitable procedures to implement this Law outside the Kingdom.	
Draft Executive Regulation of the Personal Data Protection Law (March 2022)	Personal	**Draft Executive Regulation on Personal Data** Article 28 – Transfer of Personal Data to Outside the Kingdom. Article 28.1 requires data localization within Saudi Arabia, and prohibits storage or processing outside of Saudi Arabia "before conducting an impact assessment and obtaining the written approval of the Regulatory Authority after the Regulatory Authority has liaised with the Competent Authority on a base-by-case basis". Article 28.2 permits data transfers on the basis of consent or for purposes relating to the public interest. Article 29 - Criteria and Guarantees for Personal Data Transfer to a Country not on the Approval List. This Article addresses risk and impact assessments for countries not on the "approved" list. This Article outlines several governmentally approved transfer mechanisms, including standard contractual clauses (Art. 29.b.2.a), binding corporate rules (Art. 29.b.2.b), codes of conduct (Art. 29.b.2.c), certification (Art. 29.b.2.d), or other government-approved mechanisms. Article 30 - Adequacy List. This Article requires the Competent Authority to prepare a list of the countries that provide adequate level of protection for Personal Data and the rights of Data Subjects. Excerpt: Chapter VII: Transfer or Disclosure of Personal Data to Parties outside the Kingdom Article 28 - Transfer of Personal Data to outside the Kingdom 1. The Controller shall store and process Personal Data within the geographical boundaries of the Kingdom. Personal Data may not be stored or processed outside the Kingdom before conducting an impact assessment and obtaining the written approval of the Regulatory Authority after the Regulatory Authority has liaised with the Competent Authority on a base-by-case basis. 2. In addition to the purposes stated in Article 29 of the Law, Personal Data may be transferred to outside the Kingdom for the following purposes: a. Providing services directly to individuals if providing such services requires the transfer of Personal Data to outside the Kingdom, in a manner that is not contrary to the expectations of the individuals, and provided such individuals have given their consent in accordance with the consent procedures stated in this Regulation. b. Purposes relating to the public interest. 3. Except where it is extremely necessary to save the Data Subject's life outside the Kingdom or preserve the Data Subject's vital interests, or avoid, examine or treat an infection, the Controller shall apply to the Competent Authority before transferring or disclosing Personal Data to any entity outside the Kingdom, in accordance with Article 29 of the Law. The said application shall not be valid unless the following conditions are satisfied: a. The application shall be made at least 30 days before the date proposed for starting the transfer of the data to outside the Kingdom. b. The application shall include the following:	Draft Executive Regulation on Data Protection (March 2022), https://istitlaa.ncc.gov.sa/en/transportation/ndmo/pdpl/Documents/Draft%20of%20the%20Executive%20Regulation%20of%20Personal%20Data%20Protection%20Law%20-%20MARCH%2009.pdf

Title	Types of Data Covered	Selected Rules in Saudi Arabia on Cross-Border Data Transfers or Data Localization	Sources
		(1) The Controller's name, address and registration number; and the country to which the data is to be transferred and in which the party to which the data is to be disclosed is located. (2) The purpose(s) of transferring the data to outside the Kingdom or the purpose(s) of disclosing the data. (3) The legal grounds based on which the data is to be transferred to outside the Kingdom or disclosed. (4) Categories description of the Personal Data Subjects and their Personal Data or the categories of the Personal Data belonging to such Personal Data Subjects (5) The entities to which the Personal Data is to be transferred or disclosed. c. The Competent Authority shall examine all the applications within 30 days of receiving each application. The Competent Authority may extend that period, including where the Competent Authority requests additional information from the Controller. Article 29 - Criteria and Guarantees for Personal Data Transfer to a Country not on the Approval List When transferring Personal Data to a country that is not on the approval list referred to in Article 30 of this Regulation, the Controller shall: 1. Conduct potential risk and impact assessment of each case separately. The assessment shall take into consideration whether the Controller or Processor located outside the Kingdom (i.e. the recipient) would provide a sufficient level of protection to the rights of the Data Subjects, according to the following criteria: a. General Criteria of Assessment When assessing the level of protection of Personal Data, the Controller shall take into account the type, value, volume and sensitivity of the data to be transferred; the purpose of processing; the category of the target Data Subjects; the scope of the processing; the entities with which the data is to be shared; whether the processing will take place in a restricted or incidental manner, i.e. only for one time or a limited period, or repeatedly and regularly; the country from which the data has been collected; the stages of transfer of the data, which may pass through multiple countries; assessment of the level of Personal Data protection systems at the final destination country; and the administrative procedures and technological measures for protection of Personal Data. If the protection assessment results, based on the foregoing criteria, show high risks to the rights of Personal Data Subjects, the Controller shall conduct an impact assessment based on the special criteria. b. Special Criteria of Assessment: The Controller, when assessing the country to which the data is sought to be transferred in terms of such country's laws and regulations that protect the rights of Data Subjects in relation to processing of their Personal Data; adopting of international principles and standards for protection of Personal Data; adopting of codes of conduct, general practices or special standards for protection of Personal Data; or being a party to international agreements or obligations. 2. Provide appropriate safeguards to protect Personal Data and the rights of Personal Data Subjects, as follows: a. State in contracts and agreements standard clauses, approved by the Competent Authority, to restrict the transfer of Personal Data outside the Kingdom. b. If the Controller or the Processor operates within a multinational group, prepare binding internal common rules to apply to Personal Data transfers outside the Kingdom. Such rules shall be approved by the Competent Authority. The rules shall be incorporated as an appendix to contracts or service level agreements between the two parties. The consent of the Regulatory Authority shall be required if there if any other obligation binding on that Controller or Processor, or any of their respective affiliates in another country, that is likely to have an adverse effect on the safeguards provided by the binding common rules. c. Follow the rules set out in the Codes of Conduct approved by the Regulatory Authorities or the Competent Authority as an effective tool that defines the obligations of Controllers. d. Where necessary, use independent third parties to issue accreditation certificates confirming the existence of appropriate safeguards provided by external Controllers or Processors. e. Public Entities, being Controllers or Processors, shall sign a binding agreement for transfer of Personal Data. Such agreement shall include binding contractual provisions that ensure privacy of Data Subjects and protect their rights. Article 30 - Adequacy List The Competent Authority shall prepare a list of the countries that provide adequate level of protection for Personal Data and the rights of Data Subjects, provided such list shall be regularly updated based on the detected changes that affect the protection of Personal Data or the rights of Data Subjects, based on the following criteria:	

Title	Types of Data Covered	Selected Rules in Saudi Arabia on Cross-Border Data Transfers or Data Localization	Sources
		1. Existence of appropriate regulations and legislation related to protection of Personal Data and the rights of Data Subjects; and the country is a party to appropriate international agreements and obligations. 2. The country has a supervisory authority to ensure compliance with laws and legislation mentioned above. Article 31 – Exception for Kingdom's Government Entities Abroad Transfer of Personal Data to entities abroad affiliated with the government of the Kingdom shall not be subject to the provisions of Article 28 and Article 29 of this Regulation. The Competent Authority shall, in coordination with the related authorities, prepare rules for that purpose that take into account the provision of adequate protection for Personal Data, while achieving the interest sought from the transfer of data.	
Cloud Computing Regulatory Framework (published Feb. 6, 2018, effective March 8, 2018)	All data, including government data	Excerpt: Subscriber Content Location and Transfer Art. 3-3-8: The cloud computing service providers registered with CITC and cloud computing subscribers shall not transfer any content from the Saudi Government Data outside the Kingdom for any purposes, or in any form, whether permanently or temporarily (for example: temporary storage and backup, or similar purposes), unless it is expressly stated that it is permitted according to the laws or regulations in the Kingdom, except for this "Regulatory Framework". Art. 3-3-10: Without prejudice to their obligations stipulated in Article 3-3-7, CSPs registered with CITC must clearly inform CITC and the Cloud Subscriber in advance and get their approval, if the cloud subscribers' content will be transferred, stored, or processed outside the Kingdom, permanently or temporarily. Note: Per Art. 3-2-1, all providers of cloud based services in Saudi Arabia must register with CITC.	Saudi Arabia Communications & Information Technology Commission, Cloud Computing Regulatory Framework
Essential Cybersecurity Controls (ECC-1: 2018)	All data on government servers or on critical infrastructure	With respect to at KSA government organizations, as well as private sector organizations owning, operating, or hosting Critical National Infrastructures, any "cybersecurity managed services centers for monitoring and operations must be completely present inside the Kingdom of Saudi Arabia." (See Art. 4-1-3-2).	Saudi Arabia National Cybersecurity Authority, Essential Cybersecurity Controls (ECC-1:2018)
DRAFT Cloud Cybersecurity Controls (CCC-1: 2020) (to modify/extend ECC: 1 2018) (issued Feb. 2020)	All data on government servers or on critical infrastructure	Summary: [C]loud service providers will need to provide cloud computing services from within Saudi Arabia. This requirement extends to all systems used, including storage, processing, monitoring, support, and disaster recovery. The CCC-1:2020 also requires them, to the extent required by Saudi law, to use telecommunications infrastructure, including connectivity points, provided by operators licensed in Saudi Arabia.	Al Tamimi & Co, Saudi Arabia's draft Cloud Cybersecurity Controls

Title	Types of Data Covered	Selected Rules in Senegal on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The data protection regime in Senegal is mainly governed by the following laws and regulations: • Act No 2008-12 of 25 January 2008 Concerning Personal Data Protection ("**the Act"**) • Decree No 2008-721 of 30 June 2008 relating to the the implementation of Act No 2008-12 of 25 January 2008 Concerning Personal Data Protection ("**the implementing Decree**") • Directive ("*Circulaire*") No. 2757 of June 24, 2014, designating focal points of the CDP within the ministries taken by the Prime Minister's Office regarding the census of files relating to personal data • Act No. 2008-08 of January 25, 2008, on electronic transactions • Act no. 2016-29 dated 8 November 2016 amending the criminal code • Act. No. 10-2021 of 25th June 2021 amending the criminal code. Transfer of personal data to another country is prohibited unless the receiving country provides sufficient protection for the Data Subject's private life, liberties and fundamental rights. Countries members of the African Associations of data protection (*'Association Francophone des Autorités de Protection des Données Personnelles'*) are considered to have sufficient protection for the Data Subject's private life, liberties and fundamental rights. Other countries are assessed on case-by-case basis and on criteria including the existence of data protection law and authority responsible of data protection. A transfer to a country not offering a sufficient level of protection is possible if the transfer is timely and non-massive, if the Data Subject agrees to it or if the transfer is necessary to: • Protect the life of the Data Subjects/Holders; • Protect the public interest; • Comply with obligations allowing the acknowledgment, exercise, or defence of a legal right in court; and • Perform an agreement between the Data Subject and the Data Processor or take precontractual measures upon the request of the Data Subject. In any case, prior transferring personal data, the Data controller must inform the CDP. The information must include: • The name and address of the data sender; • The name and address of the data recipient; • The full data file and description; • The type of personal data transferred; • The number of persons concerned; • The data processing purpose; • The transfer method and frequency; • The first transfer date. (Articles 49-51 of the Act)	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=SN

Title	Types of Data Covered	Selected Rules in Senegal on Cross-Border Data Transfers or Data Localization	Sources
LAW OF 2008-12 OF JANUARY 25TH, 2008 CONCERNING PERSONAL DATA PROTECTION	Personal	Excerpt **Article 49:** The data controller cannot transfer personal data to a third country if the state provides an adequate level of protection of privacy, freedom and fundamental rights of individuals with regard to the treatment of these data are or may be subject. Before any transfer of personal data to a third country, the controller must first inform the Commission of Personal Data. Before any processing of personal data from abroad, the Commission Personal Data must first verify that the controller provides an adequate level of protection of privacy, freedom and fundamental rights of individuals with regard to the treatment under this Act. The adequacy of the level of protection provided by a controller is assessed according including security measures which are applied thereto as provided in this Act, the characteristics of the treatment, such as its purpose, duration and the nature, origin and destination of the processed data **Article 50:** The data controller may transfer personal data to a third country does not meet the conditions laid down in Article previous spot if the transfer is not massive and that the person to whom the data relate has expressly agreed to transfer or if the transfer is necessary for one of the following conditions : 1) To safeguard the life of this person ; 2) to safeguard the public interest; 3) Compliance obligations for ensuring the establishment, exercise or defense of legal claims; 4) Execution of a contract between the data controller and the person concerned, or to take steps at the request of the latter. **Article 51:** The Commission Personal Data may authorize, on the basis of a reasoned request, a transfer or a set of transfers of data to third countries which do not ensure an adequate level of protection, this when the controller provides adequate with respect to the protection of privacy, freedom and fundamental rights of the persons concerned and the exercise of the corresponding rights guarantees. **Article 42 Decree :** Pursuant to Article 49 of the Law on personal data, the controller enters in the manner set out in Article 28 of this Decree, the Commission personal data before the first data transfer to a third countries. Statement of the controller must specify : 1) The name and address of the person submitting the data; 2) The name and address of the recipient of the data; 3) The name and the description of the file; 4) Categories of personal data transferred; 5) The people involved and their approximate number; 6) The purpose of data processing carried out by the recipient; 7) Mode and frequency of planned shipments; 8) The date of the first transfer. Any change in the information reported by the controller must be declared to the Commission of personal data within fifteen working days	https://www.dataguidance.com/sites/default/files/Senegal_data_protection_law_EN_1.pdf
Migration of government data and applications to local data center	Various	A new Government data center is being built in Senegal with the aim of 'guaranteeing Senegalese digital sovereignty.' President Macky Sall this week commissioned the Diamniadio National Datacenter. All government data and applications will be migrated there, and it will host them in future. "I'm instructing the government from henceforth to migrate all state data and platforms to the data center. We have to rapidly repatriate all national data hosted out of the country," President Macky Sall said at the launch of the new facility. State-owned businesses such as national electricity company Senelec will also move their data to the center in tandem with government agencies, Sall said."With this data center, the Senegalese state will be sovereign in terms of data storage. It is a tool that will preserve our informational heritage and benefit the public administration and private companies [national and international]. Until now, the majority of our data has been stored outside, in the United States and in Asia in particular," added Cheikh Bakhoum, director of the State IT Agency.	Dan Swinhoe, Senegal to migrate all government data and applications to new

Title	Types of Data Covered	Selected Rules in Senegal on Cross-Border Data Transfers or Data Localization	Sources
			government data center, Datacenterdynamics.com (2021), https://www.datacenterdynamics.com/en/news/senegal-to-migrate-all-government-data-and-applications-to-new-government-data-center/

Serbia

Title	Types of Data Covered	Selected Rules in Serbia on Cross-Border Data Transfers or Data Localization	Sources
Law on Personal Data Protection	Personal	Excerpt VIII TRANSFER OF DATA FROM THE REPUBLIC OF SERBIA Article 53 Data may be transferred from the Republic of Serbia to a state signatory to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Data may be transferred from the Republic of Serbia to a state not signatory to the Convention from paragraph 1 of this Article, or international organisation, if in this state or international organisation regulations or contract on transfer provide for a level of data protection in accordance with the Convention. Upon the data transfer from paragraph 2 of this Article, Commissioner establishes whether conditions are met and data security measures undertaken upon data transfer from the Republic of Serbia and gives permission for transfer.	

Seychelles

Title	Types of Data Covered	Selected Rules in Seychelles on Cross-Border Data Transfers or Data Localization	Sources
LAWS OF SEYCHELLES DATA PROTECTION ACT	Personal	Excerpt Transfer prohibition notice 16. (1) If it appears to the Commissioner that a person registered as a data user or as a data user who also carries on a computer bureau proposes to transfer personal data held by him to a place outside Seychelles, the Commissioner may, if satisfied that the transfer is likely to contravene or lead to a contravention of any data protection principle, serve that person with a transfer prohibition notice prohibiting him from transferring the data either absolutely or until he has taken such steps as are specified in the notice for protecting the interests of the data subjects in question. (2) In deciding whether to serve a transfer prohibition notice, the Commissioner shall consider whether the notice is required for preventing damage or distress to any person and shall have regard to the general desirability of facilitating the free transfer of data between Seychelles and other states. (3) A transfer prohibition notice shall specify the time when it is to take effect and contain — (a) a statement of the principle or principles which the Commissioner is satisfied is or are likely to be contravened and his reasons for reaching that conclusion; and (b) particulars of the right of appeal conferred by section 17. (4) Subject to subsection (5), the time specified in a transfer prohibition notice pursuant to subsection (3) shall not be before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the notice shall not take effect pending the determination or withdrawal of the appeal. (5) If by reason of special circumstances the Commissioner considers that the prohibition notice should take effect as a matter of urgency, he may include a statement to that effect in the transfer prohibition notice, and in that event, subsection (4) shall not apply and the notice shall take effect immediately. (6) The Commissioner may cancel a transfer prohibition notice by written notification to the person on whom it was served. (7) No transfer prohibition notice shall prohibit the transfer of any data where the transfer of the information constituting the data is required or authorised by or under any enactment or required by any convention or other instrument imposing an international obligation on Seychelles. (8) Any person who contravenes a transfer prohibition notice shall be guilty of an offence but it shall be a defence for a person charged with an offence under this subsection to prove that he exercised all due diligence to avoid a contravention of the notice in question.	https://greybook.seylii.org/w/se/2003-9#!fragment/zoupio-_Toc385830841/BQCwhgziBcwMYgK4DsDWszIQewE4BUBTADwBdoAvbRABwEtsBaAfX2zgGYAOAVi44AMXACwBGAJQAaZNlKEIARUSFcAT2gByDZIiEwuBEpXgtOvQZABlPKQBC6gEoBRADJOAagEEAcgGEnkqRgAEbQpOzi4kA

Singapore

Title	Types of Data Covered	Selected Rules in Singapore on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	In disclosing or transferring personal data to onshore third parties (including affiliates), an organization should ensure that it has obtained the individual's deemed or express consent to such transfer (unless exemptions apply) and, if this was not done at the time the data was collected, additional consent will be required (unless exemptions apply). It is also a requirement under the Act for organizations to enter into written agreements with their data intermediaries to whom they transfer personal data and who process such data on behalf of the organizations. The Act also contains offshore transfer restrictions, which require an organization to ensure that the receiving organization has in place "comparable protection" to the standards set out in the Act when transferring personal data outside of Singapore. Mechanisms to achieve this include (this is not a comprehensive list): data transfer agreements (for which the Commission has released including model clauses); the individual has given consent (and provided required notices have been provided); and where transfers are considered necessary in certain prescribed circumstances (which include in connection with performance of contracts between the transferring organization and the individual, subject to certain conditions being met). An organization may apply to be exempted from any requirement prescribed under the Act in respect of any transfer of personal data out of Singapore. An exemption may be granted on such conditions as the Commission may require. The Commission has published guides to data sharing (covering intragroup and third party sharing) with practical nonbinding guidance on data transfer / sharing for organizations, as well as DPMP and DPIA guides. **(Add these guides and regulations)**	Transfer in Singapore - DLA Piper Global Data Protection Laws of the World (dlapiperdataprotection.com)
PERSONAL DATA PROTECTION ACT 2012	Personal	Excerpt PART 6 - CARE OF PERSONAL DATA Transfer of personal data outside Singapore 26.—(1) An organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act. (2) The Commission may, on the application of any organisation, by written notice exempt the organisation from any requirement prescribed pursuant to subsection (1) in respect of any transfer of personal data by that organisation. (3) An exemption under subsection (2) — (a) may be granted subject to such conditions as the Commission may specify in writing; and (b) need not be published in the Gazette and may be revoked at any time by the Commission. (4) The Commission may at any time add to, vary or revoke any condition imposed under this section.	https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P16-#pr26-

Slovakia

Title	Types of Data Covered	Selected Rules in Slovakia on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	See Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Slovenia

Title	Types of Data Covered	Selected Rules in Slovenia on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	See Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

South Africa

Title	Types of Data Covered	Selected Rules in South Africa on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The Protection of Personal Information Act 4 of 2013 (POPIA) came into effect on 1 July 2020, but there was a one year grace period within which to comply with POPIA. It is now almost fully in force. POPIA caters for two scenarios relating to the transfer of personal information, namely where a responsible party in South Africa sends personal information to another country to be processed and where a responsible party in South Africa processes personal information that has been received from outside South Africa. Receiving personal information from other countries The requirements for the processing of personal information prescribed in POPIA will apply to any personal information processed in South Africa, irrespective of its origin. Sending personal information to other countries for processing A responsible party in South Africa may not transfer personal information to a third party in another country unless: • The recipient is subject to a law, binding corporate rules or a binding agreement which: o Upholds principles for reasonable processing of the information that are substantially similar to the conditions contained in POPIA and o Includes provisions that are substantially similar to those contained in POPIA relating to the further transfer of personal information from the recipient to third parties who are in another country • The data subject consents to the transfer • The transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request or • The transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request or • The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party, or the transfer is for the benefit of the data subject and: o It is not reasonably practicable to obtain the consent of the data subject to that transfer, and o If it were reasonably practicable to obtain such consent, the data subject would be likely to give it	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=ZA
SARB	Financial	**Need to know current status and get better source** "2018: The South African Reserve Bank imposed a moratorium prohibiting the migration of domestic transaction volumes from Bankserv (South Africa's bank-owned domestic payment switch) to international payment schemes. The South African Reserve Bank enacted the moratorium after it found out that domestic South African banks planned to move more of their transactions to global payment service networks. The moratorium was to be in place until a new policy was developed and enacted"	https://www2.itif.org/2021-data-localization.pdf
		Add line re draft cloud policy	

Spain

Title	Types of Data Covered	Selected Rules in Spain on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	See Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Sri Lanka

Title	Types of Data Covered	Key Provisions / Detailed Summary	Sources
Summary	Personal	At present, Sri Lanka does not have legislation in place that exclusively addresses data protection. However, there are existing legislation, such as the Banking Act No. 30 of 1988 (as amended) which provide for the protection of data on a sectoral specific basis. Sri Lanka is however currently in the process of enacting legislation for the purpose of protecting personal data. The Ministry of Digital Infrastructure and Information Technology of Sri Lanka initially introduced the first draft for the Personal Data Protection Bill (hereinafter referred to as the "**bill**") in 2019. On the 15th of November 2021, the bill was approved by the Cabinet of Ministers of Sri Lanka and subsequently published in the Government Gazette on the 19th of November 2021. It is currently awaiting approval by the Parliament of Sri Lanka. No exact time frame has been announced as to when this will take place. When a public authority processes personal data as a controller or processor, personal data may only be processed in Sri Lanka, and shall not be processed in a third country unless the Authority in consultation with the controller or processor and the relevant regulatory or statutory body, classifies the categories of personal data which may be permitted to be processed in a third country, prescribed by the Minister pursuant to an adequacy decision. In making an "adequacy decision" the relevant written law and enforcement mechanisms in the specific country relating to the protection of personal data is taken into consideration, along with the processing criteria in that country and such other prescribed criteria relating to the processing of personal data in a third country. Any such "adequacy decision" made by the Minister will be subject to periodic monitoring of any developments in the third country that may affect the decision, and the decision may be reviewed by the Minister at least every two years. Such adequacy decision will remain in force until amended or revoked by the Minister in consultation with the Authority. A controller or processor, who is not a public authority, may process personal data: • in a third country pursuant to an adequacy decision; or • in a country, which is not a "third country prescribed pursuant to an adequacy decision", only when the controller or processor can ensure compliance with the obligations imposed under the bill. In doing so, in order to ensure compliance, a controller or processor must adopt an instrument, which may be specified by the Authority, to ensure binding and enforceable commitments of the recipient in the third country to ensure the rights of the data subjects are protected and the remedies offered by the legislation are followed.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=LK
DRAFT Bill for an Act to Provide for the Regulation of Processing of Personal Data (2021)	Personal	Article 26. Cross-border Data Flow (1) Where a public authority process personal data as a controller or processor, such personal data shall be processed only in Sri Lanka and shall not be processed in a third country, unless the Authority in consultation with, that controller or processor as the case may be and the relevant regulatory or statutory body, classifies the categories of personal data which may be permitted to be processed in a third country, prescribed by the Minister pursuant to an adequacy decision made under subsection (2). (2) (a) For the purpose of making an "adequacy decision", the Minister shall, in consultation with the Authority take into consideration the relevant written law and enforcement mechanisms relating to the protection of personal data in a third country and the application of the provisions of Part I, Part II and sections 20, 21, 22, 23, 24 and 25 of Part III of this Act, and such other prescribed criteria relating to the processing of personal data, in a third country for the purpose of cross border data flow.	The Gazette of the Democratic Socialist Republic of Sri Lanka (Nov. 25, 2021), DRAFT Bill for an Act to Provide for the Regulation of Processing of Personal Data

		(b) Any adequacy decision made by the Minister under this subsection shall - (i) be subject to periodic monitoring of the developments in a third country that may affect such decisions and the Minister may review such decision at least every two years; and (ii) remain in force until amended or revoked by the Minister in consultation with the authority. (3) A controller or processor other than a public authority may process personal data - (a) in a third country prescribed pursuant to an adequacy decision; or (b) in a country, not being a third country prescribed pursuant to an adequacy decision, only where such controller or processor ensures compliance with the obligations imposed under Part I, Part II and sections 20, 21, 22, 23, 24 and 25 of Part III of this Act. (4) For the purpose of ensuring compliance under paragraph (b) of subsection (3), a controller or processor shall adopt such instruments as may be specified by the Authority to ensure binding and enforceable commitments of the recipient in the third country to ensure appropriate safeguards to the rights of the data subjects and remedies protected by this Act.	Data Guidance Summary here

Sweden

Title	Types of Data Covered	Selected Rules in Sweden on Cross-Border Data Transfers or Data Localization	Sources
Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)	Personal	See Entry under European Union	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Switzerland

Title	Types of Data Covered	Selected Rules in Switzerland on Cross-Border Data Transfers or Data Localization	Sources
Federal Act on Data Protection	Personal	Excerpt **Art. 611** Cross-border disclosure 1 Personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection. 2 In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad only if: a. sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad; b. the data subject has consented in the specific case; c. the processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party; d. disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts; e. disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject; f. the data subject has made the data generally accessible and has not expressly prohibited its processing; g. disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules that ensure an adequate level of protection. 3 The Federal Data Protection and Information Commissioner (the Commissioner, Art. 26) must be informed of the safeguards under paragraph 2 letter a and the data protection rules under paragraph 2 letter g. The Federal Council regulates the details of this duty to provide information.	https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/en

Title	Types of Data Covered	Selected Rules in Thailand on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The Data Controller may not use or disclose Personal Data without consent unless it has been exempted from the consent requirement (i.e. on the grounds of other legal bases of processing). The recipient of the Personal Data must not disclose the Personal Data for any other purposes other than as previously notified to the Data Controller when requesting for the Personal Data. In the event that the Data Controller uses or discloses Personal Data which is exempt from the consent requirement (i.e. other legal basis of processing), the Data Controller must maintain a record of such use or disclosure in the manner prescribed under the PDPA, for example the record must be kept in a written or electronic format. Processing between Data Controllers and Data Processors As the Data Processor will be carrying out activities only pursuant to the instructions given by the Data Controller, the PDPA imposes an obligation on the Data Controller to ensure that there is a data processing agreement in place between the Data Controller and Data Processor governing the activities of the Data Processor. Cross-Border Transfer Personal Data may not be transferred outside of Thailand, unless the recipient country or international organisation has adequate personal data protection standards in the Regulator's view and the transfer is in accordance with the rules prescribed by the Regulator. Exemptions may apply such as in the following cases: • the data subject has given consent and proper notification has been given by the Data Controller; • the transfer is necessary for the performance of a contract between the Data Controller and data subject; or • the transfer is necessary in order to protect the vital interests of the data subject. Transfer between group companies may be exempt from the above requirement if the international transfer is to an organisation within the same group/affiliated business and such transfer is for joint business operations. Nevertheless, the personal data protection policy of such group companies must be approved by the Regulator. The transfer requirements may have an impact on multinational organisations that routinely transfer data cross border. However, given that many organisations in Europe will already comply with similar (and likely more stringent) data protection laws, the impact of the PDPA may be limited regarding cross-border transfer of data.	
Personal Data Protection Act, B.E. 2562 (2019)	Personal	Excerpt: Part 3 - Use or Disclosure of Personal Data Section 27 The Data Controller shall not use or disclose Personal Data without the consent of the data subject, unless it is the Personal Data which is collected without requirement of consent under Section 24 or Section 26. The Person or juristic person who obtains Personal Data as a result of the disclosure under paragraph one shall not use or disclose such Personal Data for any purpose other than the purpose previously notified to the Data Controller in the request to obtain such Personal Data. In the event that the Data Controller uses or discloses the Personal Data which is exempted from consent requirement in paragraph one, the Data Controller shall maintain a record of such use or disclosure in the record under Section 39. Section 28 In the event that the Data Controller sends or transfers the Personal Data to a foreign country, the destination country or international organization that receives such Personal Data shall have adequate data protection standard, and shall be carried out in accordance with the rules for the protection of Personal Data as prescribed by the Committee in Section 16(5), except in the following circumstances: (1) where it is for compliance with the law; (2) where the consent of the data subject has been obtained, provided that the data subject has been informed of the inadequate Personal Data protection standards of the destination country or international organization; (3) where it 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; (4) where it is for compliance with a contract between the Data Controller, and other Persons or juristic persons for the interests of the data subject; (5) where it is to prevent or suppress a danger to the life, body, or health of the data subject or other Persons, when the data subject is incapable of giving the consent at such time; or (6) where it is necessary for carrying out the activities in relation to substantial public interest. In the event that there is a problem with regard to the adequacy of Personal Data protection standards of the destination country or international organization, such problem shall be submitted to the Committee to decide. The decision made by the Committee may be reviewed when there is a new evidence convincing that the destination country or international organization that receives such Personal Data has developed adequate Personal Data protection standard	https://www.dataguidance.com/sites/default/files/entranslation_of_the_personal_data_protection_act_0.pdf or https://www.dataguidance.com/sites/default/files/entranslation_of_the_personal_data_protection_act_0.pdf

Title	Types of Data Covered	Selected Rules in Thailand on Cross-Border Data Transfers or Data Localization	Sources
		Section 29 In the event that the Data Controller or the Data Processor who is in the Kingdom of Thailand has put in place a Personal Data protection policy regarding the sending or transferring of Personal Data to another Data Controller or Data Processor who is in a foreign country, and is in the same affiliated business, or is in the same group of undertakings, in order to jointly operate the business or group of undertakings. If such Personal Data protection policy has been reviewed and certified by the Office, the sending or transferring of Personal Data to a foreign country, which is in accordance with such reviewed and certified Personal Data protection policy, can be carried out and shall be exempt from compliance with Section 28. The Personal Data protection policy, the nature of the same affiliated undertaking or affiliated business in order to jointly operate the undertaking or business, and the rules and methods for the review and certification in paragraph one shall be as prescribed and announced by the Committee. In the absent of a decision by the Committee in accordance with Section 28, or the Personal Data protection policy referred in paragraph one, the Data Controller or the Data Processor may send or transfer the Personal Data to a foreign country in exemption to compliance with Section 28, if the Data Controller or the Data Processor provides suitable protection measures which enable the enforcement of the data subject's rights, including effective legal remedial measures according to the rules and methods as prescribed and announced by the Committee.	

Togo

Title	Types of Data Covered	Selected Rules in Togo on Cross-Border Data Transfers or Data Localization	Sources
Loi No. 14/2019 relativbe a la protection des donnees a caractere personnelle (In French)	Personal	Not excerpted or summarized due to lack of translation.	https://jo.gouv.tg/sites/default/files/JO/JOS_29_10_2019-64E%20ANNEE-N%C2%B026%20TER.pdf#page=1

Trinidad and Tobago

Title	Types of Data Covered	Selected Rules in Trinidad and Tobago on Cross-Border Data Transfers or Data Localization	Sources
REPUBLIC OF TRINIDAD AND TOBAGO Act No. 13 of 2011	Personal	Excerpt Commissioner to publish list of equivalent jurisdictions **28.** The Commissioner shall by Order publish in the Gazette and at least two newspapers in daily circulation in Trinidad and Tobago a list of countries which have comparable safeguards for personal information as provided by this Act. Disclosure of personal information outside of Trinidad and Tobago **46.** (1) Where personal information under the custody and control of a public body is to be disclosed to a party residing in another jurisdiction, the public body shall inform the individual to whom it relates of— (a) the purpose for which the information is being collected once that purpose is known to the public body; and (b) the identity of— (i) the person requesting the information; and (ii) the relevant public body with responsibility for Data Protection in the other jurisdiction, and obtain his consent before disclosing the information. (2) Where a person under subsection (1) does not consent to the release of his personal information, the public body shall not so disclose. (3) Subsections (1) and (2) shall not apply where the circumstances set out in section 41 exist, but personal information may be limited where the public body determines that the jurisdiction to which the personal information is being sent does not have comparable standards (4) Where a person under subsection (1) consents to the release of his information and the public body is— (a) satisfied that the jurisdiction to which the information is being sent has comparable safeguards, as provided by this Act, the public body shall disclose the personal information; or (b) not satisfied that the jurisdiction to which the information is being sent has comparable safeguards, the public body shall refer the matter to the Commissioner for a determination as to whether the other jurisdiction has comparable safeguards as provided by this Act and inform the individual to whom the personal information relates, of the referral. (5) Upon a referral under subsection (4)(b), the Commissioner shall make a determination whether the other jurisdiction has or does not have comparable safeguards as provided by this Act, and inform the public body accordingly. (6) Where the public body is informed that the jurisdiction to which the information is being sent— (a) has comparable safeguards, the public body shall inform the person concerned and disclose the personal information; (b) does not have comparable safeguards, the public body shall inform the person concerned and obtain his consent for the disclosure— (i) without limitation; or (ii) with limitation on the information sharing to the extent necessary to ensure the protection of personal privacy and information.	http://www.ttparliament.org/legislations/a2011-13.pdf

Tunisia

Title	Types of Data Covered	Selected Rules in Tunisia on Cross-Border Data Transfers or Data Localization	Sources
Organic Act n°2004-63 of July 27th 2004 on the protection of personal data	Personal	Excerpt Chapter IV - The communication and transfer of personal data **Article 47:** The communication of personal data to third parties without the express consent of the data subject, his heirs or his tutor, given by any means that leaves a written trace, is prohibited, except when the data is necessary for public authorities missions, for public security or national defense, for criminal prosecutions or for carrying out missions in accordance with the laws and regulations in force. The "Instance" may authorize the communication of personal data in case of written and explicit refusal of data subject, his heirs or his tutor whenever the communication is necessary for the protection of the data subject's life, or for scientific or historic researches, or for the performance of a contract at which the data subject is a part under the condition that the part whose personal data are communicate shall commit to take all required guarantees for the protection of data and linked rights, in accordance with the directives of the "Instance" and also under the condition that personal data shall not be used on other purposes for which they have been communicated. The provisions of article 28 of the hereby Act shall apply if the data subject is a child. **Article 48:** The authorization applying shall be submitted to the "Instance" within one month from the date of the data subject's refusal to communicate his personal data to third parties. The "Instance" shall issue its decision within one month from the date of receipt of the application. The "Instance" shall inform the applicant within fifteen days from the date of its decision by registered letter with acknowledgement on receipt or any other means that leave a written trace. **Article 49:** The personal data processed for specific aims may be communicated for being processed later for historical or scientific purposes, under the condition of the data subject's consent, his heir or his tutor and the authorization of the "'Instance Nationale de Protection des Données à Caractère Personnel". According to the cases, the "Instance" shall decide to remove or to leave the data susceptible to identify the data subject. The provisions of article 28 of the hereby Act shall apply if the data subject is a child. **Article 50:** In any cases, the transfer of personal data to a foreign State is prohibited whenever it may endanger public security or Tunisia's vital interests. **Article 51:** The transfer to a foreign State of personal data which are under processing or bound to be under processing may not take place if this State does not provide an adequate level of protection, in reference with the kind and the purposes of the data and the period of its processing and the foreign State where the data shall be transferred and the precautions which have been taken for data safety. In every cases, the transfer of personal data must be carried out in accordance with the conditions set by the hereby Act. **Article 52:** In every case, the authorization of the "Instance" is required before the transfer of personal data. The "Instance" shall issue its decision within one month from the date of receipt of the application. The application is introduced before the juvenile and family court judge whenever the personal data subject to transfer refers to a child.	https://media2.mofo.com/documents/The+Organic+Act+2004-63.pdf

Turkey

Title	Types of Data Covered	Selected Rules in Turkey on Cross-Border Data Transfers or Data Localization	Sources
Presidential Decree on Information and Communication Security Measures, No. 2019/12 (July 6, 2019)	Health, population, communications data	Summary: This measure covers a wide array of data (described as "critical data") encompassing information relating to population, health, communication records and genetic, biometric data are deemed critical data. Critical data is defined broadly to cover “information that could threaten national security or disrupt public order when its’ privacy, integrity or accessibility is compromised.” The Decree stipulates the following: • Critical data shall be stored domestically in a secure manner. • Critical data in public institutions and organizations shall be kept in a secure environment closed to the internet access, and the devices used in that secure environment shall be strictly controlled. • The data of the public institutions and organizations shall not be stored in a cloud service. • Confidential data shall not be shared or communicated through mobile applications or social media except for national mobile applications developed by authorized institutions for coded and encrypted communication. • No mobile devices or devices for data transfer shall be allowed in environments where confidential data and documents are located or where interviews are conducted. • The safety measures shall be determined for transfer of confidential data processed by public institutions and organizations. • The settings of public institutions’ e-mail systems shall be configurated securely and the servers shall be kept domestically. The communication between servers shall be made in cryptical way. The operators authorized to provide communication services shall be liable to establish an internet exchange point in Turkey. Measures shall be taken to prevent the cross-border transmission of domestic communication traffic which needs to be exchanged domestically.	Gurulkan Cakir, New Presidential Decree on Information and Communication Security Measures
Banking Information Systems and Electronic Banking Services Regulation (Official Gazette No. 31069, March 15, 2020)	Financial	Summary: “The Regulation addresses the sharing and cross-border transfer of client information. Save for the exceptions under the Banking Law, banks cannot transfer or disclose to any third parties in Turkey or abroad any information that can be regarded as clients secrets that banks acquired, stored or processed through information systems during the performance of their activities and the procurement of outsourced services, without the client's request in written form, or that is verifiable through permanent data storage. Clients' explicit consent for the disclosure of personal data cannot be a precondition for the provision of the services.”	Esin Law, New Regulation on Bank IT Systems and Electronic Banking Services
Communiqué on Information Systems Management numbered VII-128.9 (January 5, 2018)	Financial	Summary: The communique imposes data localization requirements specifying that any companies subject to independent audit will be required to maintain their primary and secondary IT systems within the territory of Turkey.	Eryulekli, Communiqué published by capital markets board on information systems management Erdem & Erdem, Management of Information Systems
Banking Law No. 5411, Privacy-related Amendments (2020)	Financial	Summary from ESIN Law: The Banking Law No. 5411 (“Banking Law”) was amended, altering banks’ data privacy practice (“Amendments“). The Amendments were published in the Official Gazette on February 25, 2020 and entered into force on the same date • Per Article 73, customer secrets may not be disclosed or transferred to any third party located in Turkey or abroad without a request or instruction from the customer, even if the explicit consent of the customer is collected in line with the Data Protection Law. The only exemptions to this rule are the mandatory legal provisions in other laws and information that must be disclosed to certain ministries listed in Article 73.	ESIN Law, Data Privacy Amendments to Turkish Banking Law

Title	Types of Data Covered	Selected Rules in Turkey on Cross-Border Data Transfers or Data Localization	Sources
		• Further, the Board of the Banking Regulatory and Supervisory Authority is authorized to prohibit the transfer of customer secrets or bank secrets to third parties abroad after it assesses the customer secret's economic security, and may render a decision ordering banks to retain their information systems and their back-ups in Turkey. • Disclosures and transfers of customer and banking secrets, including disclosures and transfers made based on the exemptions provided in the Article, must be made to the extent they are limited with the specified purposes and are proportionate. • The Board is authorized to determine the scope, method, principles and procedures related to the disclosures and transfers of customer secrets and introduce limitations related to these.	
Law on the Protection of Personal Data, No. 6698 (April 7, 2016)	Personal	Excerpt: Transfer of personal data **ARTICLE 8**- (1) Personal data cannot be transferred without explicit consent of the data subject. (2) Personal data may be transferred without seeking explicit consent of data subject upon the existence of one of the conditions provided for in: (a) the second paragraph of Article 5, (b) the third paragraph of Article 6, provided that sufficient measures are taken. (3) Provisions of other laws concerning transfer of personal data are reserved. Transfer of personal data abroad **ARTICLE 9-** (1) Personal data cannot be transferred abroad without explicit consent of the data subject. (2) Personal data may be transferred abroad without explicit consent of the data subject provided that one of the conditions set forth in the second paragraph of Article 5 and the third paragraph of Article 6 exist and that; (a) sufficient protection is provided in the foreign country where the data is to be transferred, (b) the controllers in Turkey and in the related foreign country guarantee a sufficient protection in writing and the Board has authorized such transfer, where sufficient protection is not provided. (3) The Board determines and announces the countries where sufficient level of protection is provided. (4) The Board shall decide whether there is sufficient protection in the foreign country concerned and whether such transfer will be authorised under the sub-paragraph (b) of second paragraph, by evaluating the followings and by receiving the opinions of related public institutions and organizations, where necessary: a) the international conventions to which Turkey is a party, b) the state of reciprocity concerning data transfer between the requesting country and Turkey, c) the nature of the data, the purpose and duration of processing regarding each concrete, individual case of data transfer, ç) the relevant legislation and its implementation in the country to which the personal data is to be transferred, d) the measures guaranteed by the controller in the country to which the personal data is to be transferred, (5) In cases where interest of Turkey or the data subject will seriously be harmed, personal data, without prejudice to the provisions of international agreements, may only be transferred abroad upon the permission to be given by the Board after receiving the opinions of related public institutions and organizations. (6) Provisions of other laws concerning the transfer of personal data abroad are reserved.	Turkey, Law on the Protection of Personal Data IAPP, GDPR Match-up: Turkey's Data Protection Law DLA, Data Protection Laws of the World - Turkey OneTrust, Turkey summary

Turkmenistan

Title	Types of Data Covered	Selected Rules in Turkmenistan on Cross-Border Data Transfers or Data Localization	Sources
Law on Information on Private Life and its Protection No. 519-V (in Russian)	Personal	Not excerpted or summarized due to lack of translation.	https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/107056/131641/F419973633/519.pdf

Uganda

Title	Types of Data Covered	Selected Rules in Uganda on Cross-Border Data Transfers or Data Localization	Sources
The Data Protection and Privacy Act, 2019	Personal	Excerpt **19.** Processing personal data outside Uganda. Where a data processor or data controller based in Uganda processes or stores personal data outside Uganda, the data processor or data controller shall ensure that, (a) the country in which the data is processed or stored has adequate measures in place for the protection of personal data at least equivalent to the protection provided for by this Act; or (b) the data subject has consented.	https://www.dataguidance.com/sites/default/files/data_protection_and_privacy_act_2019_1.pdf

Ukraine

Title	Types of Data Covered	Selected Rules in Ukraine on Cross-Border Data Transfers or Data Localization	Sources
Summary	Personal	The Law of Ukraine No. 2297 VI 'On Personal Data Protection' as of June 1, 2010 (Data Protection Law) is the main legislative act regulating personal data protection in Ukraine. On December 20, 2012, the Data Protection Law was substantially amended by the Law of Ukraine, 'On introducing amendments to the Law of Ukraine' 'On Personal Data Protection' dated November 20, 2012, No. 5491-VI. Additional significant changes to Data Protection Law were introduced by the Law of Ukraine 'On Amendments to Certain Laws of Ukraine regarding Improvement of Personal Data Protection System' dated July 3, 2013, No. 383-VII which came into force on January 1, 2014. In accordance with Data Protection Law, personal data may be transferred to foreign parties when there is an appropriate level of protection of personal data in the respective state of the transferee. Pursuant to the Data Protection Law, such states include member states of the European Economic Area and signatories to the EC Convention on Automatic Processing of Personal Data. The list of the states ensuring an appropriate level of protection of personal data will be determined by the Cabinet of Ministers of Ukraine. Personal data may be transferred abroad based on one of the following grounds: • Unambiguous consent of the personal data subject • Cross-border transfer is needed to enter into or perform a contract between the personal data owner and a third party in favor of the data subject • Necessity to protect the vital interests of the data subject • Necessity to protect public interest, establishing, fulfilling and enforcing of a legal requirement • Non-interference in personal and family life of the data subject, as guaranteed by the data owner	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=UA
On Personal Data Protection (Official Bulletin of the Verkhovna Rada of Ukraine (BVR), 2010, No. 34, Art. 481)	Personal	Excerpt (machine translated) **Article 29. International cooperation and personal data transfer** 1. Cooperation with foreign subjects of relations associated with personal data shall be regulated by the Constitution of Ukraine, this Law, other regulatory legal acts and international treaties of Ukraine. 2. If an international treaty of Ukraine ratified by the Verkhovna Rada of Ukraine establishes other regulations than those stipulated by the law of Ukraine, the regulations of the international treaty shall be applied. 3. Transfer of personal data to foreign subjects of relations associated with personal data is carried out only given that the relevant state ensures adequate personal data protection in cases established by law or an international treaty of Ukraine. Member states of the European Economic Area, as well as states that have signed the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, are recognised to ensure an adequate level of personal data protection. The Cabinet of Ministers of Ukraine determines the list of states that ensure proper personal data protection. Personal data may not be disseminated for any purpose other than that for which it was collected. 4. Personal data may be transferred to foreign subjects of relations associated with personal data, also in the case of: 1) granting by the personal data subject an unambiguous consent to such transfer; 2) requirement to conclude or execute a transaction between the personal data owner and a third party that is the personal data subject in favour of the personal data subject; 3) requirement to protect the vital interests of personal data subjects; 4) requirement to protect the public interest, establish, implement and ensure the legal requirement; 5) provision by the personal data owner of appropriate guarantees of non-interference in the personal and family life of the personal data subject.	https://zakon.rada.gov.ua/laws/show/2297-17?lang=en#Text

United Arab Emirates

Title	Types of Data Covered	Selected Rules in United Arab Emirates on Cross-Border Data Transfers or Data Localization	Sources
Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data Protection (“**PDPL**”)	Personal	The UAE’s Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data Protection (“**PDPL**”) was issued on 26 September 2021. The PDPL imposes limitations on the international transfer of Personal Data to outside of the UAE. Similar to the concept of the “adequate jurisdictions” in the EU, the Data Office is expected to approve certain territories as having sufficient provisions, measures, controls, requirements and rules for protecting privacy and confidentiality of personal data. There are also various other exceptions which exporters can rely on, although further details are awaited from the Data Office. The executive regulations to the PDPL (“**Executive Regulations**”) were due to be published within six months of the issuance of the PDPL. However as of 31 December 2022, those have not yet been published. Once the Executive Regulations are issued, organisations have a further six months from their date of the issuance in which they can adjust operations to compliance with the PDPL.	DLA Piper
Health Data Law (UAE Federal Law No. 2 of 2018 on the Use of the Information and Communication Technology in Health Fields (issued Feb. 6, 2018) (enacted May 2019)	Health	On 22 April 2020 the Federal Cabinet issued Cabinet Resolution No. 32 of 2020 concerning the Regulations Concerning the Use of the Information and Communications Technology in the Areas of Health (“**ICT in Health Fields Regulation**s”). The regulations provide further details, including on permission controls to access and use the central system, and on the storage and exchange of information on the central system. Excerpt: “Article 13- Storage and Transfer of Health Information and Data outside the State. The Health information and data related to the Health services provided in the State may not be stored, processed, generated or transferred outside the State, unless in the cases defined by virtue of a decision issued by the Health Authority in coordination with the Ministry.” The UAE ICT in Health Fields Law applies to all Competent Entities. “Competent Entity” is defined as *"Any entity in the State providing medical services, health insurance or national health insurance services, brokerage services, claims management services or electronic services in the medical field of any entity related, whether directly or indirectly, to the implementation of the provisions hereof."* “Health Information” is defined as *“The health information that were processed and were given a visual, audible or readable indication, and that may be attributed to the health sector, whether related to the health or insurance facilities or entities or to the health services beneficiaries.”*	UAE, Health Data Law Simmons & Simmons, New health data protection law in the UAE
Ministry of Health and Prevention, Ministerial Resolution 51/2021 (June 2021)	Health	Summary: “The UAE’s Ministry of Health and Prevention (MoHAP) has issued a long awaited resolution setting out exceptions to Article 13 of Federal Law No. 2 of 2019 (“Health Data Law“), which by default prohibits the transfer, storage, generation or processing of health data that relates to health services provided in the UAE (“UAE Health Data“) outside of the UAE. The Resolution sets out a list of permitted exceptions to Article 13 of the Health Data Law to permit cross-border transfers and overseas processing of UAE Health Data in 10 separate circumstances: i. Overseas treatment: where required to allow the treatment of patients overseas ii. Medical testing: data related to samples sent to laboratories outside of the UAE iii. Scientific research: data used in scientific research, subject to compliance with all UAE laws and associated standards, conditions and procedures concerning health research and the approval of the competent health authority iv. Insurance claims and coverage: data used by insurance and claims management companies to provide health insurance coverage or to process consent in accordance with their regulatory permissions, but only after obtaining consent from the relevant health service recipient / insured person v. Organisations cooperating with the UAE Government or its institutions: data required by competent organisations cooperating with the UAE Government, subject to any purpose limitations that apply to the relevant request vi. Wearables and healthcare monitoring devices: data processed by simple medical devices and tools used by members of the public to record and monitor health and vital signs (e.g. blood pressure, blood sugar and oxygen saturation) or other simple health data vii. Pharmacovigilance reporting: data related to disease prevention, treatment or diagnosis of patients which may cause side effects, adverse effects or negative effects, subject to the terms of accepted good practice	Baker McKenzie, UAE: Health Data Law - Permitted Transfers of Health Data Baker McKenzie, Interactive Guide

Title	Types of Data Covered	Selected Rules in United Arab Emirates on Cross-Border Data Transfers or Data Localization	Sources
		viii. Data approved by a health authority: any other data that an Emirate-level health authority approves for export or overseas processing provided that such data is not confidential for reasons of public safety, public interest or public health and that the disclosure of the data will not result in the disclosure of medical secrets, unless the patient provides their written consent ix. Telemedicine: data used to provide remote health services provided that the relevant physician has access to the system for a limited period and can only access the required information, the sharing of any associated medical images and reports is only sent to the competent physician and written consent is obtained from the patient x. Formal request: where the concerned person or their representative issues a formal request to the entity in question asking for their data to be transferred and processed abroad"	
30 September 2020 the UAE Central Bank issued a new Stored Value Facilities Regulation ("SVF Regulation"), repealing and replacing the Regulatory Framework for Stored Values and Electronic Payment Systems it has issued in September 2016	Financial data	<u>Central Bank's Stored Value Facilities Regulation</u> On 30 September 2020 the UAE Central Bank issued a new Stored Value Facilities Regulation ("SVF Regulation"), repealing and replacing the Regulatory Framework for Stored Values and Electronic Payment Systems it has issued in September 2016. While the SVF Regulation makes amendments to the licensing and enforcement regime for SVF (on onshore UAE only; it does not apply in, or affect, the DIFC and ADGM free zones), from a data protection perspective little has changed. The SVF Regulation applies to those providing Stored Value Facilities, which is now defined as *"a facility (other than cash) for or in relation to which a Customer, or another person on the Customer's behalf, pays a sum of money (including Money's Worth such as values, reward points, Crypto-Assets or Virtual Assets) to the issuer, whether directly or indirectly, in exchange for: (a) the storage of the value of that money (including Money's Worth such as values, reward points, Crypto-Assets or Virtual Assets), whether in whole or in part, on the facility; and (b) the "Relevant Undertaking". SVF includes Device-based Stored Value Facility and Non-device based Stored Value Facility".* An SVF Licensee must also adequately protect customer data (including customer identification and transaction records) which are required to be stored and maintained in the UAE. Such data can only be made available to the corresponding customer, the Central Bank, other regulatory authorities following prior approval of the Central Bank, or by a UAE court order. An SVF Licensee must store and retain all customer and transaction data for a period of five years from the date of the creation of the customer data, or longer if required by other laws. Article 10 of the SVF Regulation requires that customer data (including customer identification and transaction records) are required to be stored and maintained in the UAE.	
Draft Retail Payment Services Regulations	Financial data	In October 2020, the Central Bank of the United Arab Emirates published its Draft Retail Payment Services Regulations which requires all personal and payment data to be stored and maintained within the UAE.	
Regulating Telecommunications (Federal Law by Decree 3 of 2003 as amended), which includes several implementing regulations/policies enacted by the Telecommunications and Digital Government	Telecom data	In circumstances where telecommunications service providers provide subscriber information to affiliates or third parties directly involved in the supply of the telecommunications services ordered by a subscriber, the third parties are required to take all reasonable and appropriate measures to protect the confidentiality and security of the subscriber information, and use such information only as needed for the provision of the requested services. Telecommunications service providers are required to ensure that the contracts between them and any affiliate or third party holds the other party responsible for the privacy and protection of the subscriber's information (TDRA Consumer Protection Regulations v1.5, Article 20.8).	

Title	Types of Data Covered	Selected Rules in United Arab Emirates on Cross-Border Data Transfers or Data Localization	Sources
Regulatory Authority ('TDRA') in respect of data protection of telecoms consumers in the UAE.			
		Other data protection and privacy laws in the UAE The PDPL keeps intact existing data protection and privacy laws within the UAE's financial free zones, DIFC and ADGM, as well as the rules of the Dubai Health Care City, (links to our summaries are above) as well as applicable onshore laws regulating health data and banking and credit data. For this reason the data protection landscape in the UAE (and the wider GCC region) remains complex to navigate and somewhat fragmented, meaning that the application of the PDPL will need to be considered carefully. There are several UAE federal level laws that contain various provisions in relation to privacy and the protection of personal data: • Constitution of the UAE (Federal Law 1 of 1971) • Crimes and Penalties Law (Federal Law 31 of 2021, abrogating Federal Law 3 of 1987) • Federal Decree Law No. 34 of 2021 on Combatting Rumors and Cybercrimes	

Title	Types of Data Covered	Selected Rules in United Kingdom on Cross-Border Data Transfers or Data Localization	Sources
The Electronic Communications (Security Measures) Regulations 2022		Network architecture 3.—(1) A network provider must take such measures as are appropriate and proportionate to ensure— (a)except in relation to an existing part of the public electronic communications network, that the network is designed and constructed in a manner which reduces the risks of security compromises occurring, (b)in relation to an existing part of the public electronic communications network, that the part is redesigned and developed in a manner which reduces the risks of security compromises occurring, and (c)that the public electronic communications network is maintained in a manner which reduces the risks of security compromises occurring. ... (3) The duty in paragraph (1) includes in particular a duty—... (f) to take such measures as are appropriate and proportionate to ensure that the network provider— (i) is able, without reliance on persons, equipment or stored data located outside the United Kingdom, to identify the risks of security compromises occurring, (ii) is able to identify any risk that it may become necessary to operate the network without reliance on persons, equipment or stored data located outside the United Kingdom, and (iii) if it should become necessary to do so, would be able to operate the network without reliance on persons, equipment or stored data located outside the United Kingdom. Protection of certain tools enabling monitoring or analysis 5.—(1) This regulation applies in relation to a public electronic communications network or public electronic communications service if the network or service includes tools that enable— (a)the monitoring or analysis in real time of the use or operation of the network or service, or (b)the monitoring or analysis of the content of signals. (2) If the tools are stored on equipment located outside the United Kingdom, the network provider or service provider must take measures to identify and reduce the risks of security compromises occurring as a result of the tools being stored on equipment located outside the United Kingdom.	https://www.legislation.gov.uk/uksi/2022/933/contents
Data Protection Act 2018	Personal	Excerpt Transfers of personal data to third countries etc **18 Transfers of personal data to third countries etc** (1) The Secretary of State may by regulations specify, for the purposes of Article 49(1)(d) of the GDPR— (a) circumstances in which a transfer of personal data to a third country or international organisation is to be taken to be necessary for important reasons of public interest, and (b) circumstances in which a transfer of personal data to a third country or international organisation which is not required by an enactment is not to be taken to be necessary for important reasons of public interest. (2) The Secretary of State may by regulations restrict the transfer of a category of personal data to a third country or international organisation where— (a) the transfer is not authorised by an adequacy decision under Article 45(3) of the GDPR, and (b) the Secretary of State considers the restriction to be necessary for important reasons of public interest. (3) Regulations under this section— (a) are subject to the made affirmative resolution procedure where the Secretary of State has made an urgency statement in respect of them; (b) are otherwise subject to the affirmative resolution procedure.	https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

Title	Types of Data Covered	Selected Rules in United Kingdom on Cross-Border Data Transfers or Data Localization	Sources
		(4) For the purposes of this section, an urgency statement is a reasoned statement that the Secretary of State considers it desirable for the regulations to come into force without delay. CHAPTER 5 - TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES ETC Overview and interpretation **72 Overview and interpretation** (1) This Chapter deals with the transfer of personal data to third countries or international organisations, as follows— (a) sections 73 to 76 set out the general conditions that apply; (b) section 77 sets out the special conditions that apply where the intended recipient of personal data is not a relevant authority in a third country or an international organisation; (c) section 78 makes special provision about subsequent transfers of personal data. (2) In this Chapter, “relevant authority”, in relation to a third country, means any person based in a third country that has (in that country) functions comparable to those of a competent authority General principles for transfers **73 General principles for transfers of personal data** (1) A controller may not transfer personal data to a third country or to an international organisation unless— (a) the three conditions set out in subsections (2) to (4) are met, and (b) in a case where the personal data was originally transmitted or otherwise made available to the controller or another competent authority by a member State other than the United Kingdom, that member State, or any person based in that member State which is a competent authority for the purposes of the Law Enforcement Directive, has authorised the transfer in accordance with the law of the member State. (2) Condition 1 is that the transfer is necessary for any of the law enforcement purposes. (3) Condition 2 is that the transfer— (a) is based on an adequacy decision (see section 74), (b) if not based on an adequacy decision, is based on there being appropriate safeguards (see section 75), or (c) if not based on an adequacy decision or on there being appropriate safeguards, is based on special circumstances (see section 76). (4) Condition 3 is that— (a) the intended recipient is a relevant authority in a third country or an international organisation that is a relevant international organisation, or (b) in a case where the controller is a competent authority specified in any of paragraphs 5 to 17, 21, 24 to 28, 34 to 51, 54 and 56 of Schedule 7— (i) the intended recipient is a person in a third country other than a relevant authority, and (ii) the additional conditions in section 77 are met. (5) Authorisation is not required as mentioned in subsection (1)(b) if— (a) the transfer is necessary for the prevention of an immediate and serious threat either to the public security of a member State or a third country or to the essential interests of a member State, and (b) the authorisation cannot be obtained in good time. (6) Where a transfer is made without the authorisation mentioned in subsection (1)(b), the authority in the member State which would have been responsible for deciding whether to authorise the transfer must be informed without delay. (7) In this section, “relevant international organisation” means an international organisation that carries out functions for any of the law enforcement purposes **74 Transfers on the basis of an adequacy decision**	

Title	Types of Data Covered	Selected Rules in United Kingdom on Cross-Border Data Transfers or Data Localization	Sources
		A transfer of personal data to a third country or an international organization is based on an adequacy decision where— (a) the European Commission has decided, in accordance with Article 36 of the Law Enforcement Directive, that— (i) the third country or a territory or one or more specified sectors within that third country, or (ii) (as the case may be) the international organisation, ensures an adequate level of protection of personal data, and (b) that decision has not been repealed or suspended, or amended in a way that demonstrates that the Commission no longer considers there to be an adequate level of protection of personal data. **75 Transfers on the basis of appropriate safeguards** (1) A transfer of personal data to a third country or an international organization is based on there being appropriate safeguards where— (a) a legal instrument containing appropriate safeguards for the protection of personal data binds the intended recipient of the data, or (b) the controller, having assessed all the circumstances surrounding transfers of that type of personal data to the third country or international organisation, concludes that appropriate safeguards exist to protect the data. (2) The controller must inform the Commissioner about the categories of data transfers that take place in reliance on subsection (1)(b). (3) Where a transfer of data takes place in reliance on subsection (1)— (a) the transfer must be documented, (b) the documentation must be provided to the Commissioner on request, and (c) the documentation must include, in particular— (i) the date and time of the transfer, (ii) the name of and any other pertinent information about the recipient, (iii) the justification for the transfer, and (iv) a description of the personal data transferred **76 Transfers on the basis of special circumstances** (1) A transfer of personal data to a third country or international organisation is based on special circumstances where the transfer is necessary— (a) to protect the vital interests of the data subject or another person, (b) to safeguard the legitimate interests of the data subject, (c) for the prevention of an immediate and serious threat to the public security of a member State or a third country, (d) in individual cases for any of the law enforcement purposes, or (e) in individual cases for a legal purpose. (2) But subsection (1)(d) and (e) do not apply if the controller determines that fundamental rights and freedoms of the data subject override the public interest in the transfer (3) Where a transfer of data takes place in reliance on subsection (1)— (a) the transfer must be documented, (b) the documentation must be provided to the Commissioner on request, and (c) the documentation must include, in particular— (i) the date and time of the transfer, (ii) the name of and any other pertinent information about the recipient, (iii) the justification for the transfer, and (iv) a description of the personal data transferred. (4) For the purposes of this section, a transfer is necessary for a legal purpose if— (a) it is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) relating to any of the law enforcement purposes, (b) it is necessary for the purpose of obtaining legal advice in relation to any of the law enforcement purposes, or (c) it is otherwise necessary for the purposes of establishing, exercising or defending legal rights in relation to any of the law enforcement purposes.	

Title	Types of Data Covered	Selected Rules in United Kingdom on Cross-Border Data Transfers or Data Localization	Sources
		Transfers to particular recipients **77 Transfers of personal data to persons other than relevant authorities** (1) The additional conditions referred to in section 73(4)(b)(ii) are the following four conditions. (2) Condition 1 is that the transfer is strictly necessary in a specific case for the performance of a task of the transferring controller as provided by law for any of the law enforcement purposes. (3) Condition 2 is that the transferring controller has determined that there are no fundamental rights and freedoms of the data subject concerned that override the public interest necessitating the transfer. (4) Condition 3 is that the transferring controller considers that the transfer of the personal data to a relevant authority in the third country would be ineffective or inappropriate (for example, where the transfer could not be made in sufficient time to enable its purpose to be fulfilled). (5) Condition 4 is that the transferring controller informs the intended recipient of the specific purpose or purposes for which the personal data may, so far as necessary, be processed. (6) Where personal data is transferred to a person in a third country other than a relevant authority, the transferring controller must inform a relevant authority in that third country without undue delay of the transfer, unless this would be ineffective or inappropriate. (7) The transferring controller must— (a) document any transfer to a recipient in a third country other than a relevant authority, and (b) inform the Commissioner about the transfer. (8) This section does not affect the operation of any international agreement in force between member States and third countries in the field of judicial co operation in criminal matters and police co-operation. Subsequent transfers **78 Subsequent transfers** (1) Where personal data is transferred in accordance with section 73, the transferring controller must make it a condition of the transfer that the data is not to be further transferred to a third country or international organization without the authorisation of the transferring controller or another competent authority. (2) A competent authority may give an authorisation under subsection (1) only where the further transfer is necessary for a law enforcement purpose. (3) In deciding whether to give the authorisation, the competent authority must take into account (among any other relevant factors)— (a) the seriousness of the circumstances leading to the request for authorisation, (b) the purpose for which the personal data was originally transferred, and (c) the standards for the protection of personal data that apply in the third country or international organisation to which the personal data would be transferred. (4) In a case where the personal data was originally transmitted or otherwise made available to the transferring controller or another competent authority by a member State other than the United Kingdom, an authorisation may not be given under subsection (1) unless that member State, or any person based in that member State which is a competent authority for the purposes of the Law Enforcement Directive, has authorised the transfer in accordance with the law of the member State. (5) Authorisation is not required as mentioned in subsection (4) if— (a) the transfer is necessary for the prevention of an immediate and serious threat either to the public security of a member State or a third country or to the essential interests of a member State, and (b) the authorisation cannot be obtained in good time. (6) Where a transfer is made without the authorisation mentioned in subsection (4), the authority in the member State which would have been responsible for deciding whether to authorise the transfer must be informed without delay.	

Title	Types of Data Covered	Selected Rules in United Kingdom on Cross-Border Data Transfers or Data Localization	Sources

Uruguay

Title	Types of Data Covered	Selected Rules in Uruguay on Cross-Border Data Transfers or Data Localization	Sources
Summary		Under Data Protection Act Law No. 18.331 (11 August 2008); Decree No. 414/009 (31 August 2009) and Decree 64/2020 (17 February 2020), personal data can only be transferred to a third party: • for the compliance of purposes directly related to the legitimate interest of the transferring party and the transferee; and • with the previous consent of the data subject (i.e. the individual whose data is being transferred). Such consent may be revoked. Additionally, the data subject must be informed of the purpose of the transfer as well as of the identity of the transferee. The previous consent of the data subject would not be necessary when the individual's data to be transferred is limited to: name, surname, identity card number, nationality, address, and date of birth. The purpose and proper identification of the transferee must be included in the consent communication that would be addressed to the data subject. Evidence of the data subject's consent must be kept in the files of the data processor. If the data subject's consent is not obtained within ten business days (counted from the receipt of the communication from the data processor asking for the consent), it will be construed that the data subject did not consent to the transfer of the data. Upon the transfer, the data processor will remain jointly and severable liable for the compliance of the transferee obligations under the Data Protection Act. The Data Protection Act forbids the transfer of personal data to countries or international entities which do not provide adequate levels of data protection (according to URCDP). However, the Data Protection Act allows international transfer to unsafe countries or entities, when the data subject consents to the transfer (such consent must be given in writing), or when the guarantees of adequate protection levels arise from "contractual clauses", and "self regulation systems". The international data transfer agreement must establish the same levels of protection which are effective under the laws of Uruguay. In the case of a cross-border transfer within a group of companies, Uruguayan laws establish that the international transfer will be lawful without any authorisation whenever the branch has the same conduct code duly registered before the local URCDP. The international transfer of personal data between headquarters and their respective branches or subsidiaries is authorised when the headquarters and their branches have a conduct code duly filed before URCDP.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=UY
Personal Data Protection Law (Published Aug. 18, 2008), as amended in Law No. 19.438 (Oct. 14, 2016)	Personal	Excerpt (Machine translation) **Article 23** Data transferred internationally.- The transfer of personal data of any kind is prohibited with countries or international organizations that do not provide adequate levels of protection according to the standards of International or Regional Law in the matter. The prohibition shall not apply in the case of: (1) International judicial cooperation, according to the respective international instrument, whether Treaty or Convention, having regard to the circumstances of the case. (2) Exchange of data of a medical nature, when required by the treatment of the affected person for reasons of public health or hygiene. (3) Bank or stock exchange transfers, in relation to the respective transactions and in accordance with the legislation that results from them applicable.	https://www.impo.com.uy/bases/leyes/18331-2008

Title	Types of Data Covered	Selected Rules in Uruguay on Cross-Border Data Transfers or Data Localization	Sources
		(4) Agreements within the framework of international treaties in which the Republic of Uruguay is a party. (5) International cooperation between intelligence agencies for the fight against organized crime, terrorism and drug trafficking. It will also be possible to carry out the international transfer of data in the following circumstances: (A) That the interested party has given his unequivocal consent to the planned transfer. (B) That the transfer is necessary for the execution of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken at the request of the interested Party. (C) That the transfer is necessary for the celebration or execution of a contract concluded or to be concluded in the interest of the person concerned, between the controller and a third party. (D) That the transfer is necessary or legally required for the safeguarding an important public interest, or for the recognition, exercise or defence of a right in judicial proceedings. (E) That the transfer is necessary for the safeguarding of the vital interests of the interested party. (F) That the transfer takes place from a registry that, by virtue of laws or regulations, is designed to provide information to the public and be open to consultation by the general public or by any person who can demonstrate a legitimate interest, provided that the conditions established by law for consultation. Without prejudice to the provisions of the first paragraph of this Article, the Regulatory and Control Unit for the Protection of Personal Data may authorise a transfer or series of data transfers personal to a third country which does not ensure an adequate level of protection, where the controller offers guarantees sufficient with regard to the protection of privacy, rights and fundamental freedoms of individuals, as well as with regard to the exercise of the respective rights.	

Uzbekistan

Title	Types of Data Covered	Selected Rules in Uzbekistan on Cross-Border Data Transfers or Data Localization	Sources
Law on Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan (April 16, 2021)	Personal	Summary: "On April 16, 2021, Uzbekistan's Law on Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan entered into force. This law, which Uzbek President Shavkat Mirziyoyev signed into law on January 14, 2021, amends the country's Law on Personal Data and introduces new requirements on personal data localization. According to the new law, the personal data of Uzbek citizens must be processed "[b]y technical means physically located in the territory of Uzbekistan, and in databases duly registered with the data protection authority in Uzbekistan"—namely, the State Inspectorate for Control in the Field of Informatization and Telecommunications of the Republic of Uzbekistan (UzComNazorat). Furthermore, the data localization requirement applies to the collection, systematization, and storage of data, and to all types of data processing, including operations carried out using information technology and via the internet. (Art. 27(1).) The compliance obligation rests with the owner and/or operator of the database. The owner is any person who owns the database that includes the personal data. The operator is any person who processes the personal data."	Uzbekistan Official Gazette, *Law on Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan* US Library of Congress, *Uzbekistan: New Requirements for Uzbek Citizens' Personal Data Localization Enter into Force*
LAW OF THE REPUBLIC OF UZBEKISTAN Personal Data (Adopted by the Legislative Chamber on April 16, 2019 Approved by the Senate on June 21, 2019)	Personal	Excerpt **Article 15**. Cross-border transfer of personal data Cross-border transfer of personal data is the transfer of personal data by the owner and (or) operator outside the territory of the Republic of Uzbekistan. Cross-border transfer of personal data is carried out on the territory of foreign states that provide adequate protection of the rights of personal data subjects. Cross-border transfer of personal data to the territory of foreign states that do not provide adequate protection of personal data may be carried out in the following cases: - the subject's consent to the cross-border transfer of his personal data; - the need to protect the constitutional order of the Republic of Uzbekistan, the protection of public order, the rights and freedoms of citizens, the health and morality of the population; provided for by international treaties of the Republic of Uzbekistan. Cross-border transfer of personal data may be prohibited or restricted in order to protect the foundations of the constitutional order of the Republic of Uzbekistan, morality, health, rights and legitimate interests of citizens of the Republic of Uzbekistan, to ensure the defense of the country and the security of the state.	https://lex.uz/docs/4396428?otherlang=4

Vietnam

Title	Types of Data Covered	Selected Rules in Vietnam on Cross-Border Data Transfers or Data Localization	Sources
Summary		The Cybersecurity Law requires that domestic or foreign cyberspace service providers carrying out activities of collecting, exploiting / using, analysing and processing data being personal information, data about service users' relationships and data generated by service users in Vietnam must store such data in Vietnam for a specified period to be stipulated by the Government. In particular, according to Article 26 of the Draft Cybersecurity Decree, domestic and foreign enterprises providing telecoms and online services to customers in Vietnam may be required to locally store certain customer-related data in Vietnam for a certain period prescribed by law if the authority alerts them that their services/online platforms have been used to commit violations of Vietnam's laws but such online service providers fail to remedy the situation upon the request of the authority. According to the latest version of the Draft Cybersecurity Decree, the organizations which could be subject to the foregoing data localization requirements only include those engaging in the following services: (i) telecommunications; (ii) data storage and sharing in cyberspace; (iii) supply of national or international domains to service users in Vietnam; (iv) E-commerce; (v) online payment; (vi) intermediary payment; (vii) transport connection via cyberspace; (viii) social networking and social media; (ix) online electronic games; and (x) providing, managing or operating other information in cyberspace in the form of messages, phone calls, video calls, email or online chats.	https://www.dlapiperdataprotection.com/index.html?t=transfer&c=VN&c2=
The Law on Cybersecurity No. 24/2018/QH14 dated June 12, 2018	Personal	Excerpt (IKIGAI LAW) Cross-border data flows Domestic and foreign cyberspace service providers who collect/process/use/analyse personal data (including the data generated by service users and about their relationships) in Vietnam must store this personal information in Vietnam for a period that will be specified by the government. Any foreign enterprise that is covered under provision, must have a branch office in Vietnam. The government can frame regulations to provide further clarity to this provision. Newspaper reports indicate that the Ministry will be narrowing the reach of these provisions – thus, for an entity to be subject to data localisation norms, it will have to additionally fulfil the following three conditions: - The company provides services on telecom networks, the internet, and cyber space; - The company collects/analyses/processes personal information and user-generated data in Vietnam, and - The company has been notified that its services have been used to violate Vietnamese law, but has not taken any action or has resisted/obstructed government investigation. Since the scope of the above two conditions is very broad, this condition plays an important role in actually limiting the scope of the data localisation requirement. The Draft Decree requires the cross-border transfer of personal data to be registered, although the term 'registration' has not been defined. If registration is interpreted as requiring government approval for transfer, it would impede the free flow of data	https://www.ikigailaw.com/data-protection-in-vietnam/#_ftnref26
Decree 53 to Implement the Law on Cybersecurity	Various	On October 1, 2022, On August 15, 2022, the Ministry of Public Security (MPS) published the final Decree No. 53/2022/ND-CP (Decree 53) to implement *inter alia* the restrictive cross-border data elements of 2019 Vietnam's Cybersecurity Law. Decree 53 requires storage of data within Vietnam by "domestic enterprises," a term that has been broadly construed to include various foreign-invested enterprises and/or their subsidiaries. Decree 53 provides guidance that will enable regulators to enforce the data localization and local office requirements under Article 26 of the Cybersecurity Law. Chapter V of Decree 53 set out key provisions relating to data storage in Vietnam. Notably, Decree 53 sets out: a) Types of data subject to local storage (Article 26): o Personal data of service users in Vietnam o User-generated data in Vietnam (i.e., account name of service user, time of service use, credit card information, email address, network address (IP) of most recent login/log out, registered phone number associated with the account or data); o Data on the relationship of service users in Vietnam with onshore and offshore entities doing business in Vietnam (i.e., friends and groups with which users connect or interact). b) Local storage and local office requirements:	

Title	Types of Data Covered	Selected Rules in Vietnam on Cross-Border Data Transfers or Data Localization	Sources
		o Domestic enterprises: All domestic enterprises, no matter which services they provide, must store regulated data in Vietnam. o Foreign enterprises: There are 10 businesses/services of foreign enterprises subject to storage of regulated data in Vietnam and establishment of branches or representative offices in Vietnam ("regulated services"). These include (i) telecom services; (ii) services of data storage and sharing in cyberspace (cloud storage); (iii) supply of national or international domain names to service users in Vietnam; (iv) e-commerce; (v) online payment; (vi) intermediary payment; (vii) service of transport connection via cyberspace; (viii) social networking and social media; (ix) online electronic games; (x) services of providing, managing, or operating other information in cyberspace in the form of messages, phone calls, video calls, email, or online chat. o Conditions triggering data localization for foreign enterprises: Failure to comply/inadequately complied with written requests made by the Department of Cybersecurity and High-Tech Crime Prevention and Control under the Ministry of Public Security for Cybersecurity Law violations. Data storage period (Article 27): The time period starts from the time an entity receives a request for local storage; the minimum period being 24 months.	
Draft Amendments to Telecom Law	Various	Article 75.1 of the draft law states as follows: "Enterprises engaged in data center service and cloud computing service business are responsible for storing data in Vietnam in accordance with relevant laws."	
Draft Personal Data Protection Decree	Personal	The Draft PDPD imposes restrictions on cross-border data transfer (including registration of transferring personal data from Vietnam to foreign countries). In particular, according to the Draft PDPD, subject to a specific exemption and prior approval from the Personal Data Protection Commission ("**PDPC**"), before transferring personal data of Vietnamese citizens out of Vietnam, the following four conditions must be fulfilled: (i) consent must be obtained from the data subjects; (ii) the original data must be stored in Vietnam; (iii) the data transferor must have proof that the recipient country has personal data protection at a level equal to or higher than the level specified in the Draft PDPD; and (iv) a written approval for transfer must be obtained from the PDPC via registration procedures. Moreover, the Draft PDPD also requires a personal data controller/processor that transfers data abroad to build a system to store data transfer history for three years. As of January 2023, the draft PDP Decree is reportedly still pending at the National Assembly Standing Committee while lawmakers await the Central Politburo's comments.	
Cybersecurity Administrative Penalties	Various	On September 23, 2021, MPS released a draft Decree on Administrative Penalties in the field of Cybersecurity. The draft details various infractions to the draft PDPD, which include the transfer of data across borders.	
Circular 24	Various	According to Circular 24, electronic general information pages and social networks as entities licensed in Vietnam must use at least one domain name ".vn" and store information in servers identified by IP addresses in Vietnam.	

Zimbabwe

Title	Types of Data Covered	Selected Rules in Zimbabwe on Cross-Border Data Transfers or Data Localization	Sources
DATA PROTECTION ACT (No. 5/2021)	Personal	Excerpt **PART VII -** Transborder Flow **28 Transfer of personal information outside Zimbabwe** (1) Subject to the provisions of this Act, a data controller may not transfer personal information about a data subject to a third party who is in a foreign country unless an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data is transferred solely to allow tasks covered by the competence of the controller to be carried out. (2) The adequacy of the level of protection afforded by the third country or international organisation in question shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; with particular consideration being given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the recipient third country or recipient international organisation, the laws relating to data protection in force in the third country or international organisation in question and the professional rules and security measures which are complied with in that third country or international organisation. (3) The Authority shall lay down the categories of processing operations for which and the circumstances in which the transfer of data to countries outside the Republic of Zimbabwe is not authorised. (4) The Minister responsible for the Cyber security and Monitoring Centre in consultation with the Minister, may give directions on how to implement this section with respect to transfer of personal information outside of Zimbabwe. **29 Transfer to country outside Zimbabwe which does not assure adequate level of protection** (1) A transfer or a set of transfers of data to a country outside Zimbabwe which does not assure an adequate level of protection may take place in one of the following cases— (a) the data subject has unambiguously given his or her consent to the proposed transfer; (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; (c) the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the controller and a third party in the interest of the data subject; (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; (e) the transfer is necessary in order to protect the vital interests of the data subject; (f) the transfer is made from a register which, according to acts or regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the case at hand	https://www.dataguidance.com/sites/default/files/data_protection_act_5_of_2021.pdf