Ferracane, Martina F.

Working Paper

Restrictions on cross-border data flows

ECIPE Working Paper, No. 01/2017

Provided in Cooperation with:
European Centre for International Political Economy (ECIPE), Brussels

Suggested Citation: Ferracane, Martina F. (2017) : Restrictions on cross-border data flows, ECIPE Working Paper, No. 01/2017, European Centre for International Political Economy (ECIPE), Brussels

This Version is available at:
https://hdl.handle.net/10419/174853

ECIPE WORKING PAPER ▪ No. 1/2017

Restrictions on Cross-Border data flows: a taxonomy

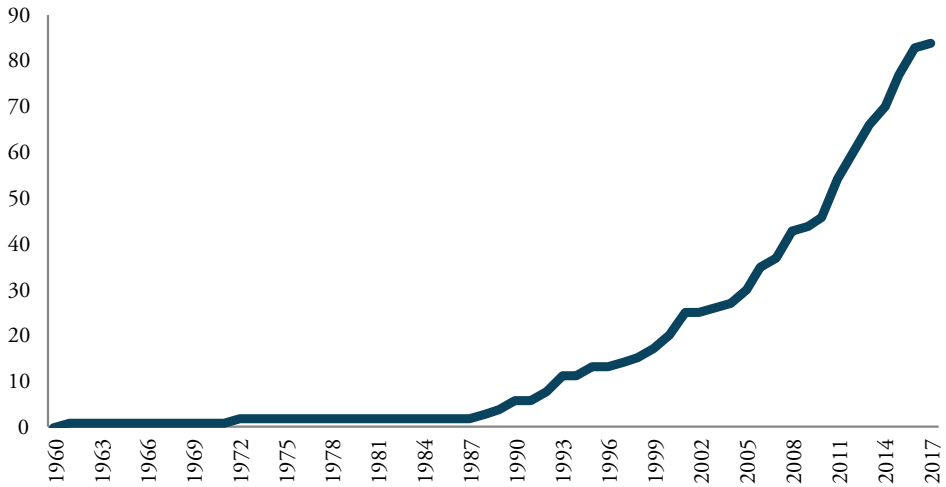
By Martina F. Ferracane, Research Associate at ECIPE and PhD student at Hamburg University

ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

1. RESTRICTIONS ON DATA FLOWS ON THE RISE[1]

Restrictions on cross-border data flows are not new, but they have mushroomed in the last decade (Figure 1). Strict privacy regimes, requests to use local data centres and outright bans to transfer data abroad are a few examples of policies imposed recently that restrict data from crossing national or regional borders.

Figure 1: Cumulative Number of Restrictions on Cross-Border Data Flows (1960-2017)[2]



Source: Own calculations based on data retrieved from Digital Trade Estimates database and legal texts.

The data revolution is both the reason behind this trend and the unwanted victim of these policies. The increasing reliance on data in our economies has raised concerns among policymakers that felt the need to respond promptly to this development with new legislation. However, the novelty of the data revolution and the difficulty of policymakers to grasp its transformational impact on the economy led to responses that impose significant costs on the economy (ECIPE, 2014; ECIPE, 2016) and on foreign businesses (USITC, 2014).

The objective of this article is to propose a basic taxonomy of restrictions on cross-border data flows, which has a bearing on many areas of law, including international trade and the protection of personal information.

2. A TAXONOMY OF RESTRICTIONS ON DATA FLOWS

From a trade perspective, restrictions on data flows can be defined as all those measures that raise the cost of conducting business across borders by either mandating companies to keep data within a certain border or by imposing additional requirements for data to be transferred abroad. These measures are very different in how they are designed and implemented.

[1] I would like to thank my colleagues Hosuk Lee-Makiyama and Erik Van der Marel for the precious discussions that guided the development of this taxonomy. I am also grateful to Anupam Chander, Martin Luther King, Jr. Professor of Law at the University of California, Davis, for his helpful comments.

[2] The data refer to 64 economies. In addition to the 28 member states of the EU, the analysis covers the following countries: Argentina, Australia, Canada, Chile, China, Colombia, Costa Rica, Ecuador, Hong Kong, Iceland, India, Indonesia, Israel, Japan, Korea, Malaysia, Mexico, New Zealand, Nigeria, Norway, Pakistan, Panama, Paraguay, Peru, Philippines, Russian Federation, Singapore, South Africa, Switzerland, Taiwan, Thailand, Turkey, United States and Vietnam.

Despite their heterogeneity, restrictions on data flow share a common trait: private entities are de facto forced to keep their data locally or are bearing higher costs for sending or processing their data abroad. These requirements can be imposed by local, central or regional governments, or in certain cases by a single public entity, such as hospitals.[3]

Restrictions on cross-border data flows can be categorised as "strict" when they specifically require data to be stored locally or as "conditional" when they impose certain conditions for data to be transferred cross-border. Both cases increase the cost of data transfers and can, therefore, result in the localisation of data.

Strict and conditional restrictions to cross-border data flow can be classified as follows:

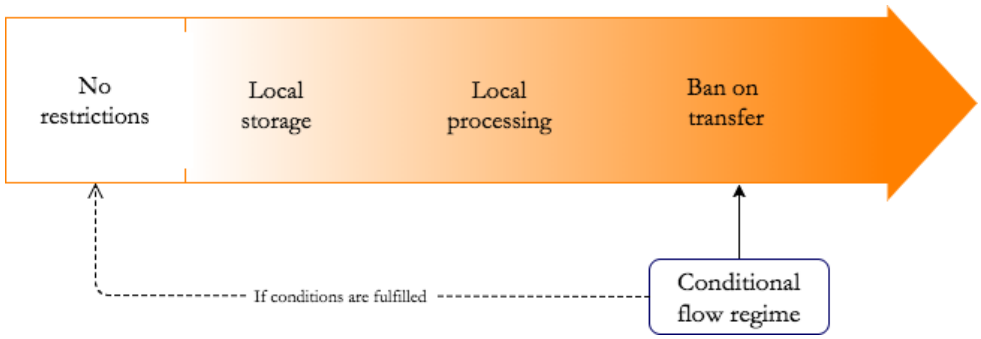
A. Strict restrictions on cross-border data flows:
   I: Local storage requirement;
   II: Local storage and processing requirement;
   III: Ban on data transfer (i.e. local storage, local processing and local access requirement).

B. Conditional restrictions to cross-border data flows:
   IV: Conditional flow regime where conditions apply to the recipient country;
   V: Conditional flow regime where conditions apply to the data controller or data processor.

Figure 2 summarises the types of restrictions on cross-border data flows from the least restrictive regime of the free flow of data across borders to the most restrictive option of a ban on the transfer of data abroad. As shown in the figure (and explained in detail below), the conditional flow regime can result in a system in which data can flow freely when the conditions are fulfilled, or in a ban on the transfer of data when the conditions are not fulfilled.[4]

While it is relatively straightforward to conclude that more restrictive measures on data imply higher costs for businesses, it is not easy to assess whether a conditional regime on data flows can be more or less costly than other regimes. This can only be assessed by looking at the specificities of the regime. In any case, the restrictiveness of any measure on trade depends on the type of data affected as well as the sectors covered by the measure.[5]

Figure 2: Types of Restrictions on Cross-Border Data Flows



[3] Obviously, when service suppliers offer to keep their customer's data locally based on commercial reasons, these do not qualify as a trade restriction.
[4] In certain cases, it is not easy to discern whether a measure is a ban to transfer, a local processing requirement or a conditional flow regime. In fact, often cases of a ban to transfer and local processing requirements have certain exceptions which could be interpreted as a conditional flow regime.
[5] For example, a measure which applies to a specific set of accounting data would usually be less restrictive for companies than a measure that applies to all personal data.

2.1. Local Storage Requirement

When a local storage requirement applies, the data cannot be transferred across borders unless a copy is stored within the borders of the country (or the jurisdiction which has imposed the requirement). In such cases, as long as a copy of the data is saved domestically, data storage and processing activities can also take place outside the country and a business can operate as usual. In most of the cases, this requirement applies to specific data such as tax and accounting records, corporate or social documents, and, in rare cases, public archives. For example, the Swedish Bookkeeping Act imposes documents such as a company's annual (financial) reports and balance sheets to be physically stored in Sweden for a period of seven years.[6]

2.2. Local Processing Requirement

In addition to local storage requirements, localisation could also extend to the processing of data. This means that the company needs to use data centres located in the country for the main processing of the data. The company is therefore required for the company to either build a data centre or to switch to local providers of data processing solutions. Alternatively, the company might decide to leave the market altogether. If this regime applies, the company can still send the data abroad, for example to the parent company, after the main processing.

Such requirements have recently been introduced in Russia, with the amendment of the Russian data protection law by the Federal Law No. 242-FZ in July 2014.[7] Article 18 §5 requires data operators to ensure that the recording, systematisation, accumulation, storage, update/ amendment and retrieval of personal data of the citizens of the Russian Federation is made using databases located in the Russian Federation.

2.3. Ban on Data Transfer

The third and most stringent type of restriction to cross-border data flows consists of a ban to transfer the data across borders. Therefore, data has to be stored, processed and accessed within the territory of the implementing country. Such policy usually applies to specific sets of data considered especially sensitive, such as health or financial data.

The difference between a ban on data transfer and a local processing requirement could be quite subtle. One might argue that storage and processing requirement taken together is de facto a ban on transfers. However, in the case of a ban on transfers, the company is not allowed to even send a copy of its data abroad, which can be important for lag-free communication between subsidiaries, or for the security of data. In both cases, however, the main data processing activities need to be done in the country.

To date, there is no country that imposes an economy-wide ban on the transfer of all data abroad, regardless of the nature of the data. However, some jurisdictions impose bans on the transfer of specific sets of data. For example, Australia requires that no personal electronic health information is held or processed outside national borders.[8] Another example is two provinces of Canada (British Columbia[9] and Nova Scotia[10]) which have enacted laws that require personal information held by public institutions (such as schools, universities, hospitals or other government-owned utilities and agencies) to stay in Canada - with only a few limited exceptions.

[6] Bokföringslag (1999:1078). December 1999.
[7] Federal law 21.07.2014 №242-FZ "On the amendment of certain legislative acts of Russian Federation concerning the procession of personal data in computer networks". July 2014. See ECIPE (2015).
[8] Section 77 of the Personally Controlled Electronic Health Record Act of 2012. Act No. 63, 2012. June 2012.
[9] Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165, s. 30.1.
[10] Personal Information International Disclosure Protection Act, S.N.S. 2006, c. 3, s. 5(1). November 2006.

2.4 Conditional Flow Regime

When a conditional flow regime is in place, the transfer of the data abroad is forbidden unless certain conditions are fulfilled. The conditions can apply to the recipient country, to the company, or to both the recipient country and the company. In most of the cases, it is enough that one of the alternative options is fulfilled in order for the company to transfer data abroad. If the conditions are stringent and cannot be fulfilled by the recipient country nor the company, the measure results in a ban on the transfer of data abroad.

The European regime of data protection is typical example of a conditional regime.[11] Under European law, conditions apply to both the recipient country and the transferring entity. In the first case, the company can transfer data abroad to countries with an "adequate level of protection".[12] In the second case, even when the recipient country is not deemed adequate, data can be transferred and processed overseas if the transferee fulfils certain conditions.

The most common condition is the consent of the data subject for cross-border transfer. This condition, as is also the case for most of the conditions, can be more or less strict, and its interpretation or enforcement may vary. For example, the General Data Protection Regulation (GDPR) requires that the data subject has "explicitly" consented to the data transfer abroad,[13] while the previous EU directive allowed controllers to rely on an "unambiguous" consent by the data subject.[14]

Alternative means to fulfil the conditions under EU law and other conditional regimes include the use of Binding Corporate Rules or the condition that the transfer is necessary to complete the contract concluded with the data subject. There are also exceptions for cases where a transfer is necessary for medical treatment, or where transfers serve the public interest; or when a transfer falls within the scope of international judicial cooperation. Also, the information transferred may already be in the public domain – e.g. already published and available legally on the internet. Any of the alternatives listed in the regulatory texts on data flows can be used by an entity as a legal basis for transferring data abroad.

A particular condition imposed in certain jurisdictions with conditional flow regimes is the infrastructure requirement. When this requirement applies, the firm must build a server locally in order to operate in the country.[15] An example of this condition is in Vietnam, where any company that wants to process data is required to build at least one server in the country "serving the inspection, storage, and provision of information at the request of competent state management agencies".[16] Also in this case, the regime could easily turn into a local processing requirement if the server has to be used to process all information managed by the data controller or data processor.

[11] The European Union is currently updating its data protection regime by replacing the Directive 95/46/EC with the General Data Protection Regulation (GDPR). The GDPR will enter into force in May 2018.
[12] As of today, 12 jurisdictions have been deemed to have an adequate level of protection: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Jersey, the Isle of Man, Israel, New Zealand, Switzerland and Uruguay. In addition, the EU/US Safe Harbour acted as a self-certification system open to certain US companies for the data protection compliance, until its invalidation by the European Court of Justice in October 2015. The system has now been replaced by the Privacy Shield.
[13] Article 49 of the General Data Protection Regulation, Regulation (EU) 2016/679. May 2016.
[14] Article 26 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[15] These requirements would be referred to as 'performance requirements' under investment law.
[16] Decree No. 72/2013/ND-CP of July 15, 2013, on the Management, Provision and Use of Internet Services and Online Information.

3. WAY FORWARD

This taxonomy of data restrictions has important implications in many policy areas, including international trade law. In fact, restrictions on data flows may affect countries' legal commitments under various trade agreements, including the General Agreement on Trade in Services (GATS).

The objectives behind these restrictions can be diverse. They include privacy, cybersecurity, national security, public order, law enforcement, taxation, and industrial development, among others. However, these objectives can be achieved with different policies, and it is legitimate to ask whether a certain type of restriction on data flows is the least trade-restrictive measure available to achieve that objective, or is even necessary to fulfil the policy objective at all.

An accurate taxonomy of the restrictions on data flows is just one piece of the puzzle needed to answer this question. Further research is needed on two areas. The first is economic, and relates to the impact of these measures on trade. It will be relevant to analyse how the costs of various restrictions or conditionalities vary, and how they affect business decisions of those entities engaged in international trade. The second area is legal, and relates to how the different restrictions in this taxonomy contribute to achieving the desired policy objective. In particular, it will be relevant to investigate certain policy objectives that fall under GATS exceptions in Art. XIV and XIV bis - such as data privacy, national security, prevention of (cyber) fraud and public order.

This future research will be paramount to assess whether restrictions on data flows are necessary to achieve a certain policy objective, or whether less trade-restrictive measures on data flows could be a suitable policy alternative to achieve the desired policy objective while complying with trade commitments.

REFERENCES

Crosby, D. (2016), "Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments". E15Initiative. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum, 2016. Available at http://e15initiative.org/wp-content/uploads/2015/09/E15-Policy-Brief-Crosby-Final.pdf

European Centre for International Political Economy (ECIPE) (2014), "The Costs of Data Localisation: Friendly Fire on Economic Recovery". Authors: M. Bauer, H. Lee-Makiyama, E. Van der Marel, B. Verschelde. March 2014. Available at http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf

European Centre for International Political Economy (ECIPE) (2015), "Data Localisation in Russia: A Self-imposed Sanction". Authors: M. Bauer, H. Lee-Makiyama, E. Van der Marel. June 2015. Available at http://ecipe.org/publications/data-localisation-russia-self-imposed-sanction/

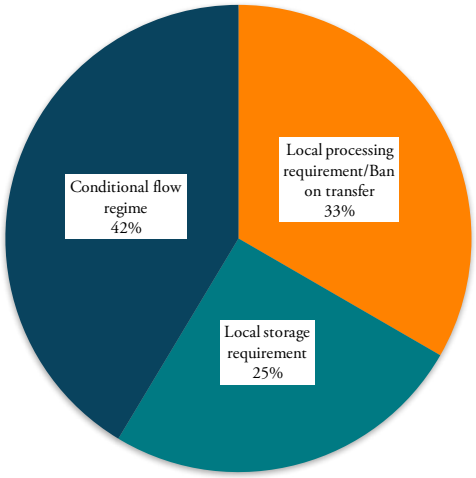
European Centre for International Political Economy (ECIPE) (2016), "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States". Authors: M. Bauer, M.F. Ferracane, H. Lee-Makiyama, E. van der Marel. March 2016. Available at http://ecipe.org//app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf

United States International Trade Commission (USITC) (2014), "Digital Trade in the U.S. and Global Economies, Part 2", August 2014. Available at https://www.usitc.gov/publications/332/pub4485.pdf

ANNEX A: ANALYSIS OF THE RESTRICTIONS TO CROSS-BORDER DATA FLOWS CURRENTLY IN FORCE

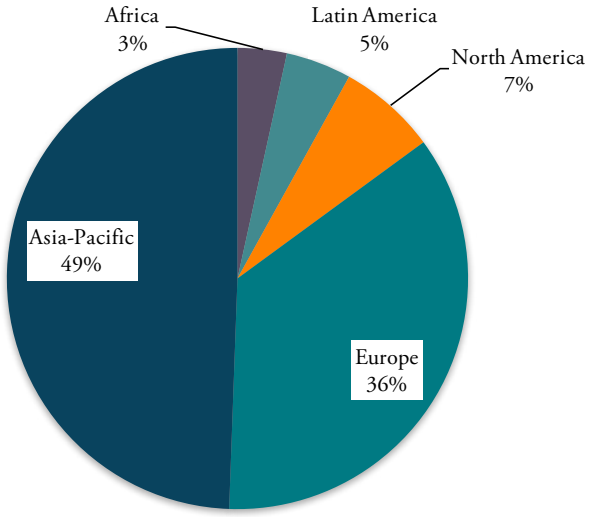
In this Annex, I present a short analysis of restrictions to cross-border data flows which are currently in force in 64 economies.[17] The analysis is based on 87 measures collected by ECIPE and available at the Digital Trade Estimates (DTE) Database: www.ecipe.org/dte/database. The measures are also listed in Annex II.

Figure A.1: Type of Restrictions to Cross-Border Data Flows (1960-2017)



Source: Own calculations based on data retrieved from DTE database and other sources

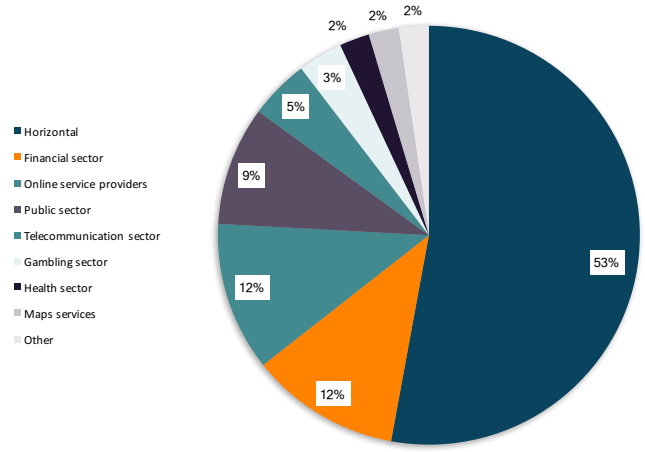
Figure A.2: Geographical Coverage of Restrictions to Cross-Border Data Flows (1960-2017)[18]



Source: Own calculations based on data retrieved from DTE database and other sources

[17] Supra Note 1.
[18] The Russian Federation is listed under 'Asia-Pacific' region.

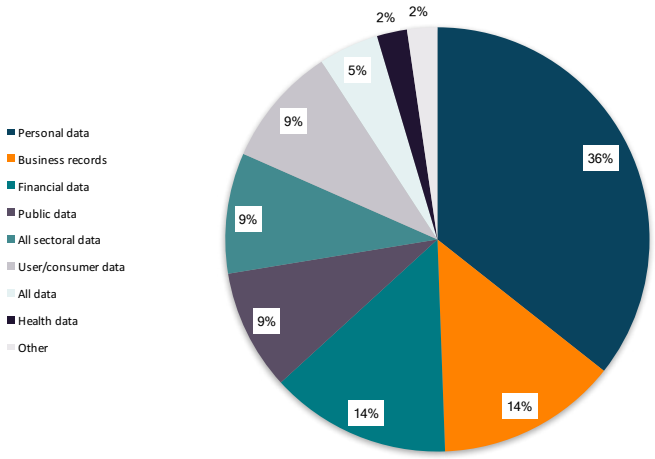
Figure A.3: Sectoral Coverage of Restrictions to Cross-Border Data Flows (1960-2017)



Source: Own calculations based on data retrieved from DTE database and legal texts

Note: While the majority of the measures are horizontal (53%), about half of the measures are sector-specific and, in particular, target the financial sector, online service providers,[19] the public sector, the telecommunication sector, the gambling sector, the healthcare sector or maps services. The data reveals that bans to transfer data and local storage requirements tend to be sector-specific, while conditional flow regimes tend to be horizontal as they apply mostly to personal data in all sectors.

Figure A.4: Type of Data Targeted by Restrictions to Cross-Border Data Flows (1960-2017)



Source: Own calculations based on data retrieved from DTE database and legal texts

Note: More than a third of all measures identified apply to personal data. They often relate to conditional flow regimes that apply horizontally to all sectors. Given the technical difficulties and costs required to separate personal data from non-personal data (especially with new advancements such as the Internet of Things (IoT), measures that apply to personal data are likely to apply de facto to all data in the economy. In addition, 14% of the measures apply to business records. In these cases, measures applied are usually local storage requirements and are implemented to facilitate access to such data by governments needed swiftly. Other data targeted are financial data (14% of the measures), public data, user data and data from an entire sector (9% of the cases each). Finally, a few measures (5%) apply to all data in the economy and 2% of measures apply to the healthcare sector.

[19] This category includes different businesses operating online from advertising companies to cloud providers.

ANNEX B: LIST OF RESTRICTIONS TO CROSS-BORDER DATA FLOWS[20]

Country	Act, practice	Description measure
Argentina	Law No. 25326 (Data Protection Act) Regulatory Decree No. 1558/2001	Section 12 of the Data Protection Act of Argentina (Law 25,326) prohibits the transfer of personal data to countries that do not have an adequate level of protection in place, but such countries have not been identified yet. The Regulatory Decree No. 1558/2001 provides that the prohibition is not applicable when the data subject has expressly consented to the transfer. Data can also be transferred to a foreign country by means of an international agreement between the data controller and the foreign processor, under which the latter undertakes to comply with the same standards of protection and other legal obligations as provided in the Argentine data protection regulations.
Australia	Personally Controlled Electronic Health Record Act of 2012 - Section 77	The Personally Controlled Electronic Health Record Act of 2012 requires local data centres to handle 'personally controlled electronic health records'. Therefore, no electronic health information can be held or processed outside Australia, unless they do not "include information in relation to a consumer" or they are "identifying information of an individual or entity".
Australia	Federal Privacy Act 1988 as amended by The Privacy Amendment (Enhancing Privacy Protection) Act 2012	Under the Federal Privacy Act, before an organisation discloses personal information to an overseas recipient, it must take reasonable steps to ensure that the overseas recipient will not breach the Australian Privacy Principles (APPs). This requirement does not apply only if: - the overseas recipient is bound by a law similar to the APPs that the data subject can enforce; - the data subject consents to the disclosure of the personal data in the particular manner prescribed by APP; or - another exception applies. An organisation may be held liable for any breaches of the APPs by that overseas recipient.
Brunei	Local storage requirement	Brunei has laws that require that data generated within the country to only be stored in servers within the country.
Canada	Personal Information International Disclosure Protection Act, S.N.S. 2006, c. 3, s. 5(1)	Nova Scotia requires that personal information held by a public body (primary and secondary school, universities, hospitals, government-owned utilities and public agencies) must be stored or accessed in Canada only. A public body may override the rules where storage or access outside of the respective province is essential. Moreover, the data can be transferred outside Canada "where the individual the information is about has identified the information and has consented, in the manner prescribed by the regulations, to it being stored in or accessed from, as the case may be, outside Canada".

[20] Source: Digital Trade Estimates (DTE) Database: www.ecipe.org/dte/database

Canada	Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165, s. 30.1	British Columbia requires that personal information held by a public body (primary and secondary school, universities, hospitals, government-owned utilities and public agencies) must be stored or accessed in Canada only. A public body may override the rules where storage or access outside of the respective province is essential. Moreover, the data can be transferred outside Canada "if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction".
Canada	Canadian Federal Law Personal Information Protection and Electronic Documents Act	According to the Canadian Federal Law Personal Information Protection and Electronic Documents Act, consent is not necessary for the transfer of data to a third country as the Canadian law does not distinguish between domestic and international transfers of data. The company should, however, grant a comparable level of protection while the information is being processed by a third party. This is, preferably, achieved on a contractual basis with the third party.
Canada	Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information	In 2006, Québec amended its Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information to require public bodies to ensure that information receives protection "equivalent" to that afforded under provincial law before "releasing personal information outside Québec or entrusting a person or a body outside Québec with the task of holding, using or releasing such information on its behalf".
Canada	Freedom of Information and Protection of Privacy Act	Alberta's Freedom of Information and Protection of Privacy Act permits the disclosure of personal information controlled by a public body in response to a "subpoena, warrant or order" only if issued by a court with "jurisdiction in Alberta".
China	Notice to Urge Banking Financial Institutions to Protect Personal Financial Information	The "Notice to Urge Banking Financial Institutions to Protect Personal Financial Information" states that the processing of personal information collected by commercial banks must be stored, handled and analysed within the territory of China, and such personal information is not allowed to be transferred overseas.
China	Administrative Measures for Population Health Information (For Trial Implementation).	Population health information needs to be stored and processed within China. In addition, storage is not allowed overseas.
China	Law of the People's Republic of China on Guarding State Secrets	The transfer of data containing state secrets abroad is prohibited.
China	Interim Measures for the Administration of Online Taxi Booking Business Operations and Services	China instituted a licensing system for online taxi companies which requires them to host user data on Chinese servers.
China	Data localisation requirement	China has data residency laws that declare companies can store the data they collect only on servers in country.
China	Map Management Regulations	Online maps are required to set up their server inside the country and must acquire an official certificate.

China	Administrative Regulations for Online Publishing Services ("Online Publishing Regulations")	Strict guidelines for what can be published online and how the publisher should conduct business in China came into force in March 2016. According to the rules, any publisher of online content, including "texts, pictures, maps, games, animations, audios, and videos" will be required to store their "necessary technical equipment, related servers and storage devices" in China.
China	Cybersecurity Law	The Cybersecurity Law includes requirements for personal information of Chinese citizens and "important data" collected by "key information infrastructure operators" (KIIOs) to be kept within the borders of China. If there are business needs for the KIIOs to transfer this data outside of China, security assessments must be conducted. The definition of KIIOs remains to be finalised.
China	Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems	Article 5.4.5. of the Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems prohibit the transfer of personal data abroad without express consent of the data subject, government permission or explicit regulatory approval "absent express consent of the subject of the personal information, or explicit legal or regulatory permission, or absent the consent of the competent authorities". If these conditions are not fulfilled, "the administrator of personal information shall not transfer the personal information to any overseas receiver of personal information, including any individuals located overseas or any organizations and institutions registered overseas". Although the Guidelines are a voluntary technical document, they might serve as a regulatory basis for judicial authorities and lawmakers.
Colombia	Law 1581 of 2012 (as regulated by decree 1377 of 2013) Law 1266 of 2008 (as regulated by decrees 2952 of 2010 and 1727 of 2009)	Pursuant to Law 1266 of 2008, personal data may not be transferred outside of Colombia to countries which do not comply with the adequate standards of data protection. This restriction does not apply in the following cases: - when there is an express authorisation by the data subject; - when the information relates to medical data as required by issues of health and public hygiene; - for banking operations; and - for operations carried out in the context of international conventions which Colombia has ratified.

EU	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data	All EU Member States follow the Data Protection Directive 95/46/EC. Under the Directive, data is freely allowed to flow outside the European Economic Area only where: - the recipient jurisdiction has an adequate level of data protection, - the controller adduces adequate safeguards (for instance, by using model contract clauses, binding corporate rules or other contractual arrangements); - the data subject has given his/her consent unambiguously; - the transfer is necessary for the performance of a contract between the data subject and the controller; - the transfer is necessary for the performance of a contract concluded in the interest of the data subject; - the transfer is justified by public interest; - the transfer is necessary to protect the vital interests of the data subject; - the data is public. The Directive has been implemented in a variety of ways in each of the 28 Member States and therefore the conditions to allow a transfer to a third country can vary. As of today, 12 jurisdictions have been deemed to have an adequate level of protection: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Jersey, the Isle of Man, Israel, New Zealand, Switzerland and Uruguay. In addition, the EU/US Safe Harbour acted as a self-certification system open to certain US companies for the data protection compliance, until its invalidation by the European Court of Justice in October 2015. The European Union is currently updating its data protection regime by replacing the Directive 95/46/EC with a Regulation (General Data Protection Regulation). The Regulation was approved in April 2016 and it will have immediate effect on all 28 EU Member States after a two-year transition period.
Belgium	Companies Code - Article	Article 463 of the Companies Code requires that the company register of shareholders and register of bonds must be kept at the registered office of the company. Since 2005, it is possible to keep the registers in electronic format as long as they are accessible at the registered office of the company.
Belgium	VAT Code - Article 60	With respect to VAT, invoices received and copies of invoices issued by the taxpayer must be stored in Belgium or in another EU member state under certain conditions. Invoices must be stored either in electronic or paper format (Article 60, § 3 of the VAT Code).
Belgium	Income Tax Code - Article 315	With respect to income tax, other than in cases of exception granted by the administration, the books and documents must be kept at the disposal of the tax administration in the office, agency, branch or other professional or private premises of the taxpayer where they have been kept, prepared or sent.

Bulgaria	Gambling Act	In Bulgaria, an applicant for a gaming license must ensure that all data related to operations in Bulgaria is stored on a server located in the territory of Bulgaria. Moreover, the applicant has to ensure that the communication equipment and the central computer system of the organiser are located within the EEA or in Switzerland.
Denmark	Consolidated Act No. 648 of 15 June 2006 (Bookkeeping Act)	The basis of the Bookkeeping Act (section 12) is that financial records must be stored in Denmark or in the Nordic countries. This applies to both physical appendixes and digital data. Hence, if financial records are stored on a server physically placed outside Denmark a complete copy must be kept in Denmark.
Denmark	Consolidated Act No. 1035 of 21 August 2007 (Audit Act)	The basis for the Audit Act (section 45) is that financial records for governmental institutions must be stored in Denmark. This applies to both physical appendixes and digital data. This regulation means that financial records may be stored on a server abroad provided that an exact copy of the records is made on a monthly basis at a minimum. Such copy must be placed on a server in Denmark or in paper.
Denmark	Consolidated Act No. 528 of 15th June 2000 as changed by Act No. 201 of 22nd March 2001 (Executive Order on Security)	Since 2011, the Danish Data Protection authority has ruled in several cases against processing of local authorities' data in third countries without using standard contractual clauses. This is the result of a strict interpretation of the European Directive 95/46/EC. Therefore, services such as Dropbox, Google Apps and Microsoft's Office 365 cannot be used by local authorities unless they have signed an agreement with the processor based on standard contractual clauses.
Finland	Accounting Act (1336/1997)	The Accounting Act requires that a copy of the accounting records in kept within Finland. Alternatively, the records can be stored in another EU country if a real-time connection to the data is guaranteed.
France	Ministerial Circular from 5 April 2016 - Note d'information du 5 avril 2016 relative à l'informatique en nuage (cloud computing)	A ministerial circular dated 5 April 2016 on public procurement states that it is illegal to use a non-"sovereign" cloud for data produced by public (national and local) administration: all data from public administrations have to be considered as archives and therefore stored and processed in France.
Germany	Act on Value Added Tax - Section 14b (Umsatzsteuergesetz, UStG)	The Act on Value Added Tax states that invoices must be stored within the country, including when stored electronically. Alternatively, in case of electric storage, they may be stored within the territory of the EU if full online access and the possibility of download are guaranteed. In this case, the entity is obliged to notify the competent tax authority in writing of the location of the electronically stored invoices, and the tax authority may access and download the data.
Germany	Tax Code - Section 146(2) 1 (Abgabenordnung, AO)	Under the Tax Code, all persons and companies liable to pay taxes that are obliged to keep books and records must keep those records in Germany. There are some exceptions for multinational companies.
Germany	German Commercial Code - Section 257 No. 1 and 4 (Handelsgesetzbuch § 257)	According to the German Commercial Code, accounting documents and business letters must be stored in Germany.

Germany	German Telecommunications Act, as amended in December 2015	Under the Directive on Data Retention, operators were required to retain certain categories of traffic and location data (excluding the content of those communications) for a period of between six months and two years and to make them available, on request, to law enforcement authorities for the purposes of investigating, detecting and prosecuting serious crime and terrorism. On 8 April 2014, the Court of Justice of the European Union declared the Directive invalid. However, not all national laws which implemented the Directive have been overturned. In 2010, the German Constitutional court found the implementation of the Directive on Data retention to be unconstitutional. Yet, in October 2015, a new data retention law was passed, which will enter into force in 2017. The law provides that telecommunication providers must retain data such as phone numbers, the time and place of communication (except for emails), and the IP addresses for either four or 10 weeks. The data is to be stored in servers located within Germany (§113b).
Greece	National law 3917/2011	In Greece, the Law No. 3971/2011 goes further in the implementation of the Data Retention Directive (later annulled by the European Court of Justice) by requiring that retained data on 'traffic and localisation' stay 'within the premises of the Hellenic territory'. The Law is still in force.
Italy	Presidential Decree No. 633 of 1972	Article 39 of the Presidential Decree no. 633 of 1972 asserts that state electric archives related to accounting data for VAT declarations may only be kept in a foreign country if some kind of convention has been concluded between Italy and the receiving country governing the exchange of information in the field of direct taxation. Therefore, such limitation does not apply intra-EU.
Luxembourg	CIRCULAR CSSF 12/552 as amended by Circulars CSSF 13/563 and CSSF 14/597	According to the Circular CSFF 12/552, financial institutions in Luxembourg are required to process their data within the country. Processing abroad is exceptionally permitted for an entity of the group to which the institution belongs or with explicit consent.
The Netherlands	Public Records Act	Localisation requirements apply to public records that have to be stored in archives in specific locations in the Netherlands. This applies both to paper and electronic records.
Poland	Polish Gambling Act	According to the Polish Gambling Act, any entity organising gambling activities is obliged to archive all data exchanged between such entity and the users in an archive device located in Poland in real time. Another restriction is the requirement that the equipment (servers) for processing and storing information and data regarding the bets and their participants must be installed and kept on the territory of a member state of the EU or EFTA.

Portugal	Data protection law	In Portugal, all transfers of data outside the EU must be notified and, except when directed to whitelisted countries or when using model contracts, they have to be authorised by the relevant Commission. On 10 November 2015, the Portuguese Data Protection Authority (DPA) also issued specific guidelines on Intra-Group Agreements ("IGA") involving transfers of personal data to non-EEA countries. The DPA considers that such transfers depend on prior authorisation for the purposes of assessing if IGAs contain sufficient guarantees that the personal data transferred continues to benefit from the same level of protection as in the EEA countries.
Romania	Law no. 124 from May 2015, regarding the approval of the Government Emergency Ordinance no. 92/2014 regulating fiscal measures and modification of laws	In Romania, the game server must store all data related to the provision of remote gambling services, including records and identification of the players, the stakes placed and the winnings paid out. Information must be stored using data storage equipment (mirror server) situated on Romanian territory.
Romania	Law on the protection of individuals with regards to the processing of personal data and the free movement of such data (Data Protection Law)	In Romania, any transfer of personal data to any state requires prior notification to the National Supervisory Authority for Personal Data Processing (NSAPDP). Moreover, any transfer of personal data to a recipient state not offering an adequate level of protection needs prior approval.
Slovenia	Slovenian Personal Data Protection Act	In Slovenia, transfers of personal data to non-EEA and non-whitelist countries require the approval of the Commissioner. The approval is issued if the Commissioner establishes that a sufficient level of protection is ensured for the transfer of personal data respectively for the data subjects to which this data relates.
Spain	Organic Law relating to Personal Data Protection	In Spain, cross-border data flows subject to Model Contracts or binding corporate rules require prior authorisation from the Director of the Spanish Data Protection Authority.
Sweden	Swedish Accounting Act (Bokföringslag (1999:1078))	In Sweden, documents such as a company's annual reports, balance sheets and annual financial reports must be physically stored in Sweden for a period of seven years.
Sweden	Local storage requirement	In relation to specific government authorities, there are certain provisions which might require the data processed by the authority to be held within Sweden or within the authority. This might affect the supply of cloud computing to public authorities.
Sweden	Local storage requirement	The Financial Services Authority requires 'immediate' access to data in its market supervision which, according to business, the supervisory body interprets as being given physical access to servers. Accordingly, Swedish financial services providers are de facto required to maintain all their records inside Swedish jurisdiction.
UK	Companies Act 2006 - Art. 388	According to the Companies Act 2006, "if accounting records are kept at a place outside the United Kingdom, accounts and returns (...) must be sent to, and kept at, a place in the United Kingdom, and must at all times be open to such inspection".

Iceland	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Act on the Protection of Privacy as regards the Processing of Personal Data No 77/2000, (amended by Acts No 90/2001, and No 81/2002)	As a member of the European Economic Area (EEA), Iceland follows the same data protection rules as the 28 European Member States. Under the Directive, data is freely allowed to flow outside the European Economic Area only where: - the recipient jurisdiction has an adequate level of data protection, - the controller adduces adequate safeguards (for instance, by using model contract clauses, binding corporate rules or other contractual arrangements); - the data subject has given his/her consent unambiguously; - the transfer is necessary for the performance of a contract between the data subject and the controller; - the transfer is necessary for the performance of a contract concluded in the interest of the data subject; - the transfer is justified by public interest; - the transfer is necessary to protect the vital interests of the data subject; - the data is public. The Directive has been implemented in a variety of ways in each of the 28 Member States and therefore the conditions to allow a transfer to a third country can vary. As of today, 12 jurisdictions have been deemed to have an adequate level of protection: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Jersey, the Isle of Man, Israel, New Zealand, Switzerland and Uruguay. In addition, the EU/US Safe Harbour acted as a self-certification system open to certain US companies for the data protection compliance, until its invalidation by the European Court of Justice in October 2015. The European Union is currently updating its data protection regime by replacing the Directive 95/46/EC with a Regulation (General Data Protection Regulation). An agreement of the final text was reached in December 2015 and the Regulation will have immediate effect on all 28 EU Member States after a two-year transition period, and on the EEA countries once the GDPR is incorporated into the EEA Agreement.
India	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules	The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules provide that cross-border data flows of sensitive personal data or information can be made: - provided that such transfer is necessary for the performance of a lawful contract between the body corporate (or any person acting on its behalf) and the provider of information, or - provided that such transfer has been consented to by the provider of information.

India	National Data Sharing and Accessibility Policy Public Records Act, No. 69 of 1993	In 2012, India enacted a "National Data Sharing and Accessibility Policy", which effectively means that government data (data that is owned by government agencies and/or collected using public funds) must be stored in local data centres. Moreover, Section 4 of the Public Records Act of 1993 already prohibited public records from being transferred out of Indian territory, except for 'public purposes'. It provides: "No person shall take or cause to be taken out of India any public records without prior approval of the Central Government: provided that no such prior approval shall be required if any public records are taken or sent out of India for any official purpose".
Indonesia	Government Regulation No. 82 of 2012 regarding the Provision of Electronic System and Transaction (Regulation 82)	Regulation 82 states that the storing of personal data and performing a transaction with the data of Indonesian nationals outside the Indonesian jurisdiction is restricted. This requirement appears to refer to personal data and transaction data of Indonesian nationals which is used within Indonesia and/or related to Indonesian nationals in particular. The Regulation targets "electronic systems operators for public services", whose definition remains unclear. In January 2014, the Technology and Information Ministry circulated a Draft Regulation with Technical Guidelines for Data Centers. The unclear and possibly all-encompassing definition of public services gave rise to concerns when a spokesperson was quoted as saying: "[the draft] covers any institution that provides information technology-based services." Data carriers covered by these provisions, therefore, would include a wide range of actors such as cloud providers, foreign banks and mobile phone providers.
Indonesia	Law No. 11 of 2008 regarding Electronic Information and Transaction Government Regulation No. 82 of 2012 regarding the Provision of Electronic System and Transaction (Regulation 82) Draft Regulation with Technical Guidelines for Data Centers	In Indonesia, data protection is covered by Law No. 11 of 2008 regarding Electronic Information and Transaction (EIT Law) and Government Regulation No. 82 of 2012 regarding the Provision of Electronic System and Transaction (Regulation 82), which went into force on 15 October 2012. Regulation 82 requires "electronic systems operators for public service" to set up a data centre and disaster recovery centre in Indonesian territory for the purpose of law enforcement and data protection. In January 2014, the Technology and Information Ministry circulated a Draft Regulation with Technical Guidelines for Data Centers. The unclear and possibly all-encompassing definition of public services gave rise to concerns when a spokesperson was quoted saying: "[the draft] covers any institution that provides information technology-based services." Data carriers covered by these provision, therefore, would include a wide range of actors such as cloud providers, foreign banks and mobile phone providers.
Indonesia	Circular Letter of Bank Indonesia No. 16/11/ DKSP Year 2014 regarding E-money Operations	In the Annex of Circular Letter of Bank Indonesia No. 16/11/DKSP Year 2014 regarding E-money Operations, there is a requirement for all operators of e-money to localise data centres and data recovery centres within the territory of Indonesia.

Indonesia	Government Regulation No. 82 of 2012 regarding the Provision of Electronic System and Transaction (Regulation 82)	In Regulation 82, there are some situations where both parties have an agreement which includes clauses relating to data transferring activity. In these situations, it is thought that this agreement is sufficient as a ground for data transferring activities. Despite this, obtaining consent would complement the requirement to minimise future complaints from the data subject.
Israel	Privacy Protection Act, 5741-1981 Privacy Protection Regulations (Transfer of Data to Databases Outside of Israel), 2001	The Privacy Protection Regulations of 2001 permit transfers to: EU Member States; other signatories of Council of Europe Convention 108; and any country "which receives data from Member States of the European Community, under the same terms of acceptance". Transfers to other countries are permitted: - subject to data subject consent; - from an Israeli corporate parent to a foreign subsidiary; or - provided the data importer enters into a binding agreement with the data exporter to comply with Israeli legal standards concerning the storage and use of data.
Japan	Act on the Protection of Personal Information (Act No. 57 of 2003; "APPI")	The Act on the Protection of Personal Information (APPI) did not originally restrict the transfer of personal information to foreign countries. Yet, recent amendments that took effect in May 2017 added cross-border transfer restrictions. The amended APPI prescribes three types of legitimate transfers of personal information to a third party in a foreign country: (1) transfers to a country that the Personal Information Protection Commission (PPC) has designated as having an acceptable level of data protection; (2) transfers to a third party in a foreign country in circumstances in which actions have been taken to ensure the same level of data protection as in Japan (such as entering into a data transfer agreement imposing obligations on the transferee meeting the requirements of the APPI); or (3) transfers with the data subject's consent.
Korea	Act on the Establishment, Management, etc. of Spatial Data - Article 16	Korea imposes a prohibition to store high resolution imagery and related mapping data outside the country and justifies this restriction on security grounds. It is reported that the prohibition led to a competitive disadvantage for international online map services, since their locally-based competitors are able to provide several services (such as turn-by-turn driving/walking instructions, live traffic updates, interior building maps) that international service providers cannot.
Korea	Personal Information Protection Act (PIPA) - Art. 17 (3)	The Personal Information Protection Act requires companies to obtain consent from data subjects prior to exporting their personal data.

Korea	Act on Promotion of Information and Communications Network Utilisation (the Network Act)	If a user's personal information is transferred to an overseas entity, the Network Act requires online service providers to disclose and obtain the user's consent, regarding 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 held by the third party, the third party's purpose of use of the personal information and the period of retention and use.
Korea	Financial Holding Company Act (FHCA)	Despite provisions in its FTAs with EU and US to allow financial data to be sent across borders, Korea prohibited outsourcing of data-processing activities to third parties in the financial services industry for several years and today certain restrictions still apply. Banks can therefore only process financial information related to Korean customers in-house, either in Korea or abroad and offshore outsourcing is restricted to a financial firm's head office, branch or affiliates. In June 2015, the Korea Financial Services Commission proposed revisions to its outsourcing policies by eliminating its requirements for (1) prior approval for the outsourcing of IT facilities; (2) offshore outsourcing to be restricted to a financial firm's head office, branch or affiliates (thus permitting use of third parties); and (3) use of a standardised outsourcing contract form (thus permitting customised contracts provided they include certain obligatory terms). Such revisions were implemented in July 2015. Yet, certain conditions for processing abroad still apply today.
Malaysia	Personal Data Protection Act 2010	The Personal Data Protection Act (PDPA) does not permit a data user to transfer any personal data out of Malaysia. However, the Act offers a set of exceptions, permitting the transfer of data abroad under certain conditions. The transfer is allowed if: - the data subject has given his consent to the transfer; - the transfer is necessary for the performance of a contract between the data subject and the data user; - the transfer is necessary for the conclusion or performance of a contract between the data user and a third party that is either entered into at the request of the data subject or in his interest; - the transfer is in the exercise of or to defend a legal right; - the transfer mitigates adverse actions against the data subjects; - reasonable precautions and all due diligence to ensure compliance to conditions of the Act were taken; or - the transfer was necessary for the protection the data subject's vital interests or for the public interest as determined by the Minister. While officially entered into force in November 2013, the PDPA has not yet been enforced.

Mexico	Federal Law for the Protection of Personal Data in the Possession of Private Parties	According to the Federal Law for the Protection of Personal Data in the Possession of Private Parties, domestic and international transfers need the consent of the individual. Additionally, the data controller must provide the third parties with the privacy notice that was sent to and consented to by the individual. Consent is not required for international transfer: - if transfer is intra-group; - if it results from a contract executed or to be executed in the interest of the data owner between the data controller and a third party; and - in few other circumstances.
New Zealand	Inland Revenue Acts	New Zealand's Inland Revenue Service issued a "Revenue Alert" stating that companies were required to store business records in data centres physically located in New Zealand in order to comply with the Inland Revenue Acts.
New Zealand	Privacy Act of 1993	Consent is not required for the transfer of data to third countries, subject to compliance with the Information Privacy Principles. However, both the Privacy Act and the Health Information Privacy Code continue to apply to personal information and health information even when it is transferred out of New Zealand. The Privacy Commissioner is given the power to prohibit a transfer of personal information from New Zealand to another state, territory, province or other part of a country by issuing a transfer prohibition notice.
Nigeria	Guidelines on Nigerian content development in information and communications technology	At the beginning of 2014, the National Information Technology Development Agency (NITDA) released guidelines on Nigerian content development in information and communications technology. One of the requirements imposes that "Data and Information Management Firms" host government data locally within the country and shall not for any reason host any government data outside the country without an express approval from NITDA and the Secretary of Federal Government. Another requirement imposes that all ICT companies host their subscriber and consumer data locally.
Nigeria	Guidelines on Point-of-Sale Card Acceptance Services	The Guidelines on Point-of-Sale Card Acceptance Services require IT infrastructure for payment processing to be located domestically. All Point-of-Sale and ATM domestic transactions need to be processed through local switches and it is forbidden to route transactions outside the country for processing.

Norway	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Personal Data Act	As a member of the European Economic Area (EEA), Norway follows the same data protection rules as the 28 European Member States. Under the Directive, data is freely allowed to flow outside the European Economic Area only where: - the recipient jurisdiction has an adequate level of data protection, - the controller adduces adequate safeguards (for instance, by using model contract clauses, binding corporate rules or other contractual arrangements); - the data subject has given his/her consent unambiguously; - the transfer is necessary for the performance of a contract between the data subject and the controller; - the transfer is necessary for the performance of a contract concluded in the interest of the data subject; - the transfer is justified by public interest; - the transfer is necessary to protect the vital interests of the data subject; - the data is public. The Directive has been implemented in a variety of ways in each of the 28 Member States and therefore the conditions to allow a transfer to a third country can vary. As of today, 12 jurisdictions have been deemed to have an adequate level of protection: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Jersey, the Isle of Man, Israel, New Zealand, Switzerland and Uruguay. In addition, the EU/US Safe Harbour acted as a self-certification system open to certain US companies for the data protection compliance, until its invalidation by the European Court of Justice in October 2015. The European Union is currently updating its data protection regime by replacing the Directive 95/46/EC with a Regulation (General Data Protection Regulation). An agreement of the final text was reached in December 2015 and the Regulation will have immediate effect on all 28 EU Member States after a two-year transition period and on the EEA countries once the GDPR is incorporated into the EEA Agreement.
Pakistan	Prohibition of data transfer	Although the transfer of data to third parties is not specifically regulated under the laws of Pakistan, data cannot be transferred to a country which is not recognised by Pakistan. Currently, the list of countries not recognised by Pakistan include: Israel, Taiwan, Kosovo, Somaliland, Nagorno-Karabakh, Transnistria, Abkhazia, Northern Cyprus, Sahrawi Arab Democratic Republic, South Ossetia and Armenia. This list may change from time to time. Furthermore, data can only be transferred to India if such a transfer can be justified by the transferor.

Peru	Law No. 29733 (Personal Data Protection Law)	In the case of cross-border transfers, the data holder must generally abstain from making transfers of personal data if the destination country does not offer 'adequate protection levels', which are equivalent to those offered by the Personal Data Protection Law or in international standards. If the destination country fails to offer adequate protection levels, the controller must guarantee that the treatment of personal data meets such requirements (for example, via a written agreement). This guarantee is not necessary if the owner of the personal data has given its prior, informed, express and unequivocal consent to the transfer or if other exceptions apply. Moreover, any cross-border data transfers must be reported to the Peruvian Data Protection Authority.
Philippines	Guidelines on Outsourcing Resolution No. 2115 of 2015 - Amendments in the Manual of Regulations for Banks and Manual of Regulations for Non-Bank Financial Institutions on the guidelines on outsourcing	According to the Circular No. 899, offshore outsourcing of bank's domestic operations is permitted only when the service provider operates in jurisdictions which uphold confidentiality. When the service provider is located in other countries, the bank should take into account and closely monitor, on continuing basis, government policies and other conditions in countries where the service provider is based during risk assessment process. The Bangko Sentral (the Central Bank of Philippines) examiners shall be given access to the service provider and those relating to the outsourced domestic operations of the bank. Such access may be fulfilled by on-site examination through coordination with host authorities, if necessary.
Russia	Federal Law no. 152-FZ "On Personal Data" (OPD-Law) as amended in July 2014 by Federal Law No. 242-FZ "On Amendments to Certain Legislative Acts of the Russian Federation for Clarification of Personal Data Processing in Information and Telecommunications Networks"	Russian data protection has been covered since 27 July 2006 by Federal Law no. 152-FZ, also known as the OPD-law ("On Personal Data"). In July 2014, the law was amended by the Federal Law No. 242-FZ to include a clear data localisation requirement. Article 18 §5 requires data operators to ensure that the recording, systematisation, accumulation, storage, update/amendment and retrieval of personal data of the citizens of the Russian Federation is made using databases located in the Russian Federation. This amendment entered into force on 1 September 2015. It is not clear how restrictive the data localisation requirement is, but it appears that the OPD-Law does not prohibit accessing the servers from abroad and does not impose any special restriction on cross-border data transfers or duplication of personal data. Online websites that violate the prohibition could be placed on the Roscomnadzor's blacklist of websites.

Russia	Federal Law No. 161-FZ "On the National Payment System" dated June 2011 (the NPS Law) as amended in October 2014 by the Federal Law No. 319-FZ "On Amendments to the Federal Law on the National Payment System and Certain Legislative Acts of the Russian Federation"	The amendments to the National Payment System Law require international payment cards to be processed locally. The law requires international payment systems to transfer their processing capabilities with respect to Russian domestic operations to the local state-owned operator (National Payment Card System) by 31 March 2015. The amendments are reported to be a response to the international political sanctions which prohibited certain international payment systems (e.g., Visa and MasterCard) from servicing payments on cards issued by sanctioned Russian banks.
Russia	New provisions in the Federal law on information, information technologies and protection of information (often referred to as Blogger's law)	The "Blogger's law" requires "organizers of information distribution in the Internet" (it is not clear which operators fall under this definition) to store on Russian territory information on facts of receiving, transfer, delivery and/or processing of voice information, texts, images, sounds and other electronic messages and information about users during six months from the end of these actions. Blogs with more than 3,000 readers are required to register as "organizers of information distribution" and are therefore subject to this requirement. Platforms that do not comply with these requirements upon a second notice face a fine of 500,000 rubles (approx. 900 USD) and can be blocked in Russia by Roscomnadzor. Russian services such as VKontakte, Yandex and Mail.Ru already registered their activities.
Russia	Government Decree No. 758 of 31 July 2014 and No. 801 from 12 August 2014	The Russian Government has given instructions to require public Wi-Fi user identification. The government decrees require that: - ISPs should identify Internet users, by means of identity documents (such as a passport); - ISPs should identify terminal equipment by determining the unique hardware identifier of the data network; - all legal entities in Russia are required to provide ISPs monthly with the list of the individuals that connected to the Internet using their network. The data should be stored locally for a period of at least six months. Later in 2015, the authorities proposed the following levels of fines for non-compliance: - 5,000-50,000 rubles (approx. 60-140 USD) for individual entrepreneurs; and - 100,000-200,000 rubles (approx. 1,400-2,600 USD) for legal entities. The fines would be higher for repeat offenders.

Russia	Federal Law no. 152-FZ "On Personal Data" (OPD-Law) of July 2006	According to the Federal Law no. 152-FZ "On Personal Data" (OPD-Law) the transfer of data outside Russia does not require additional consent from the data subject only if the jurisdiction that the personal data is transferred to ensures adequate protection of personal data. Those jurisdictions are parties to the Convention 108 and other countries approved by the Russian Federal Service for Supervision in the sphere of Telecom, Information Technologies and Mass Communications (Roskomnadzor). Roskomnadzor's official list of countries includes Australia, Argentina, Canada, Israel, Mexico and New Zealand.
Singapore	Personal Data Protection Act	An organisation may only transfer personal data outside Singapore if it has taken appropriate steps to ensure that: - it will comply with the Personal Data Protection Act (PDPA) obligations in respect to the transferred personal data while it remains in its possession or under its control; and - the recipient outside of Singapore is bound by legally enforceable obligations to provide a standard of protection to the personal data transferred that is comparable to that under the PDPA. An organisation will be taken to have satisfied the second requirement if the individual consents to the transfer of the personal data to the recipient in that country.
South Africa	Protection of Personal Information Act 4 of 2013	Consent is needed for the data transfer to third countries. Otherwise, the transfer can happen if: - the third party is subject to a law, binding corporate rules or binding agreement that provides an adequate level of protection; - the transfer is necessary for the performance of a contract between the data subject and the responsible party, or - the transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.

Switzerland	Swiss Federal Protection Act	According to the Swiss Federal Protection Act, personal data may only be transferred to countries with legislation providing for an adequate level of protection of personal data. These comprise EU Member States, whitelisted countries (currently these are Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland and Uruguay) and the U.S. for those companies or organisations who have self-certified themselves under the U.S.-Swiss "Safe Harbor" framework. If the recipient country does not have legislation providing an adequate level of data protection, one of the following conditions must be fulfilled: - the existence of a trans-border dataflow contract or other "sufficient safeguards"; - sufficient binding corporate rules; - the data subject's consent; - the export of the personal data at issue is required for the conclusion or performance of a contract with the data subject; - the export of the personal data is necessary for public interest; - the export of the personal data is necessary to protect the life or physical integrity of the data subject; or - the data subject itself has made the personal data publicly available.
Taiwan	Personal Data Protection Act (PDPA)	The transfer of personal information to mainland China is prohibited.
Taiwan	Personal Data Protection Act (PDPA) - Art. 21	There is no consent requirement for transfer in third countries, but the data subject has to be notified in advance that his/her personal data is being transferred to another country. Yet, according to Article 21 of the Personal Data Protection Act (PDPA), the international transmission of personal information can be interrupted by the central competent government authority if the transmission involves major national interests or if the country receiving personal information lacks adequate data protection laws.
Taiwan	Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation	The Financial Supervisory Commission (FSC) established stringent rules for processing of personal financial information off-shore. Yet, on May 2014, the requirements that both local and foreign banks establish standalone onshore data centres were lifted.
Turkey	Payment Services and Electronic Money Institutions Law No. 6493	Article 23 of Law No. 6493 requires that "the system operator, payment institution and electronic money institution shall be required to keep all the documents and records related to the matters within the scope of this Law for at least ten years within the country, in a secure and accessible manner". The article also specifies that "the information systems and their substitutes, which are used by system operator to carry out its activities shall also be kept within the country".

Turkey	Data Protection Law No. 6698	The legislation stipulates that data cannot be processed or transferred abroad without the individual's explicit consent. Consent will not be required if the transfer is necessary to exercise a right or is required by law, and either: - Sufficient protection exists in the transferee country, or - if the data controller gives a written security undertaking and Turkey's Data Protection Board grants permission.
Turkey	Electronic Communications Act	The transfer of traffic and location data abroad is permitted with the data subjects' explicit consent.
United States	Network Security Agreements	It is reported that foreign communications infrastructure providers have been asked to sign Network Security Agreements (NSAs) in order to operate in the US. These agreements ensure that U.S. government agencies have the ability to access communications data when legally requested. The agreements reported range in date from 1999 to 2011 and involve a rotating group of government agencies including the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), Department of Justice (DoJ), Department of Defense (DoD) and sometimes the Department of the Treasury. According to the Washington Post, the agreements require companies to maintain what amounts to an "internal corporate cell of American citizens with government clearances" ensuring that "when U.S. government agencies seek access to the massive amounts of data flowing through their networks, the companies have systems in place to provide it securely". Moreover, the agreements impose local storage requirements for certain customers data as well as minimum periods of data retention for data such as billing records and access logs.
Vietnam	Decree No. 72/2013/ND-CP of July 15, 2013, on the Management, Provision and Use of Internet Services and Online Information	The Decree No. 72 entered into force in September 2013 establishes local server requirements for online social networks, general information websites, mobile telecoms network based content services and online games services. All these organisations are required to establish at least one server inside the country "serving the inspection, storage, and provision of information at the request of competent state management agencies".
Vietnam	Decree 90/2008/ND-CP dated 13 August 2008 on anti-spam (Decree 90)	According to the Decree 90 of 2008, advertising service providers that use email advertisements and internet based text messages are required to send emails from a Vietnamese domain name (".vn") website which is operated from a server located in Vietnam.