International Privacy Laws and Related Developments – Q3 2016
(* indicates update from Q2 2016)

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
Argentina Personal Data Protection Law No. 25,326 ("PDPI")	*Personal Data* is information of any kind referred to certain or ascertain-able physical persons or legal entities. *Sensitive Data* is personal data revealing racial and ethnic origin, political opinions, religious, philosophical or moral beliefs, labor union membership, and information concerning health conditions or sexual habits or behavior	Yes, except when collected for the inherent duties of the State; or arising from special, contractual relationships that inherently grant authority	Yes, if transferee country or entity does not provide adequate levels of protection, or if for international judicial cooperation	Yes	Controlling body may apply sanctions consisting in a warning, suspension, or a fine ranging between 1,000 pesos and 100,000 pesos, based on the seriousness and extent of the violation	
Australia Privacy Amendment (Enhancing Privacy Protection) Bill 2012	Effective March 12, 2014: A single set of 13, privacy principles, Australian Privacy Principles (APPs) will apply to both private-sector and Australian government agencies. The definition of	No, as long as the entity only uses personal information for the purpose for which it was collected or for a related secondary purpose that the data subject would reasonably expect the information to be	Yes, but the transferring organization must ensure that the receiving organization overseas does not breach the APPs. Note- the transferring organization is liable	Yes	Commissioner can seek civil penalties in the event of a serious or repeated privacy breaches, max. fine for corporations is $1.7M	Reform Information: http://www.oaic.gov.au/privacy-portal/resources_privacy/Privacy_law_reform.html#news; APPs: http://www.oaic.gov.au/publications/privacy_fact_sheets/Privacy-factsheet17_Australi

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
	"personal information" in the Privacy Act 1988 (Cth) (Privacy Act) will be replaced with the following: personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable: a. whether the information or opinion is true or not; and b. whether the information or opinion is recorded in a material form or not.	used for. Where consent is required it can be either express or implied.	for any breach of the recipient.			an_privacy_principles.pdf
Australia	"Personal Information" is "information or an opinion (including information or an opinion of forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can	Yes, however, organizations may not collect sensitive data from a data subject unless: (A) the individual has consented: (B) collection is required or authorized by law; (C) the information is required to establish or defend a legal or equitable claim; (D)	Yes, Transferred outside is permissible if: (A) the transferor reasonably believes that the info is subject to a law, binding scheme or contract which effectively upholds fair handling substantially similar to Australia's National Privacy Principles (NPPs); (B)	Yes	Complaint process through Commissioner; fines range from AUD10,000 to AUD40,000.	

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	reasonably be ascertained, from the information or opinion." "Sensitive Information" means (A) information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record that is also personal information; (B) health information about an individual; or (C) genetic information about an individual that is not otherwise health information.	the individual is incapable of consenting and the information is needed because of a serious and imminent threat to the life or health of the data subject; or (E) if collected by a non-profit organization.	the data subject consents; (C) necessary for the performance of a contract between the data subject and the transferor; (D) necessary for the performance of a contract concluded in the interest of the data subject between the transferor and a third party; or (E) when 3 requirements are met: (i) transfer is in data subject's interest, (ii) it is impractical to obtain their consent, and (iii) they would be likely to give their consent; or (F) transferor has taken reasonable steps to ensure info is used by transferee consistent with the NPPs.			

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
Australia*	The Australian Federal Parliament said it plans to have a long-proposed mandatory data breach notification law enacted by the end of its current session, which runs until Dec. 1. Australia currently has no law requiring companies that fall victim to a data breach to notify the government or affected individuals. The proposed law, which is an amendment to the Australian Privacy Act 1988, requires all entities subject to the Privacy Act, including governmental agencies, to notify the Office of Australian Information Commissioner as well as any affected individuals of serious data breaches, and states that the notification must occur "as soon as practicable" after the entity becomes aware of the incident. The law defines serious breaches as those that involve the compromising of: • Personal information • Credit reporting information • Credit eligibility • Tax file number information				It specifies a maximum penalty of $1.8 million for non-compliance.	Proposed bill: https://www.ag.gov.au/consultations/pages/serious-data-breach-notification.aspx
Brazil No Comprehensive Statute						Internet Privacy Law (Law No. 12.965) extends a constitutional right to privacy to the Internet. Internet service providers must preserve user connection data for six months, but will not be held liable for content posted by users. The law also guarantees net neutrality and provides that offensive content can only be removed by court order (with some exceptions).

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
						http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm
Canada Personal Information Protection and Electronic Documents Act ("PIPEDA")	Personally identifiable information about an identifiable individual. Generally does NOT include name, title, business address, or telephone number of an employee or organization.	Yes. Verbal and/or implied consent is OK, though some evidence should be kept. Consent must be obtained at the time the data is collected.	Yes	Yes	Complaint process through Commissioner, most complaints settled before getting to that stage.	
Canada PIPEDA Amendment Bill S-4	"Personal information" means information about an identifiable individual. Companies must notify affected individuals in the event of loss, unauthorized access to or unauthorized disclosure of personal information resulting from breach of a company's security safeguards or from a failure to establish safeguards.	Yes. Consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.	Yes	Yes	Failures to comply with breach notice obligations subject to fines of up to C$100,000 per individual who wasn't informed. Failures to keep records or covering up data breaches may be subject to fines of up to C$100,000 per offense.	Bill S-4 is currently proposed legislation that would amend PIPEDA: http://www.parl.gc.ca/content/hoc/Bills/412/Government/S-4/S-4_1/S-4_1.PDF

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
	If a breach could be reasonably believed to create a real risk of significant harm to an individual, it must be disclosed to the Commissioner in a report detailing the nature of the breach.					
Cayman Islands	Data relating to a data subject and includes an expression of opinion about a data subject and any indication of the intentions of the data controller or any other person in respect of a data subject	Yes, notable exemption for corporate finance purposes	Unclear	Yes, data subjects may request the data controller to rectify, block, erase or destroy inaccurate data	Yes, a conviction on criminal indictment has a $25,000 fine, and a summary conviction has a conviction of $10,000	http://www.dataprotection.ky/images/downloads/general%20public%20consultation%20paper.pdf
China Standing Committee Decision on Strengthening Protection of Internet Data	Not specifically defined, but related to "private affairs" including any type of personal information relating to individuals.	The consent of the data subject should be obtained for the collection and use of personal data; it is prohibited to collect data regarding the religious or political opinions of any individual.	Yes, so long as the consent of the data subject has been obtained and the effect of the transfer does not harms the interests of the State, cause social instability or substantially infringe any data subject's rights.	No	Yes, administrative penalties (e.g., warning, confiscation of illegal income, fines, revoking business licensure, etc.) may be imposed. For serious violations, criminal penalties including imprisonment for up to 20 days.	English Translation available: http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403445_text

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
China Provisions on the Protection of Personal Information of Telecommunications and Internet Users	Information collected by a telecommuni-cations or internet service provider and can be used alone or combined with other information to identify a user. Includes name, date of birth, ID card number, address, telephone number, account name and password, as well as "meta information" about a user's habits, including the time and location of the use of the services.	Must obtain consent before collecting and using personal information	Unknown	Unknown	Administrative warnings, fines of up to RMB 30,000, and criminal penalties	
China*	China published its new Interim Measures for the Administration of Operation and Services of E-hailing Taxis, a series of rules designed to regulate e-hailing services, and ensure the protection of driver and passenger data. The measures include a data localization requirement that stipulates operators of e-hailing platforms must locate their servers within mainland China, and that any personal information collected or business data generated during operations must be stored and used only within China, and retained for two years. In addition, operators must also disclose the purpose, method and scope of their data collection and their use of personal driver or passenger data. They must also refrain from: • Using personal data without consent of the data subjects. • Sending personal data to third parties (unless for the purposes of a criminal investigation). • Disclosing information related to national security. Under the new law, e-hailing services must also adopt cybersecurity and other technical measures to protect data, as well as disclose any data breaches of personal information "without delay."			Yes	Fines for illegal data use or disclosure range from RMB 2,000 to RMB 10,000, and violators can also be liable to civil penalties or criminal sanctions.	Full text of measures (in Chinese): http://zizhan.mot.gov.cn/zfxxgk/bnssj/zcfgs/201607/t20160728_2068633.html

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
Colombia Ley 1581 del 17 de Octubre de 2012 por el cual se Dictan Disposiciones Generales para la Protección de Datos Personales (the "Act")	"Personal data: is information relating to an identified natural person.	Prior, informed consent required. Consent may be revoked. Data subject must be informed of: the data collected; the purpose of collection; the identity and address of the data controller; and the data subject's rights to access, correction, and revocation of consent.	Consent required unless destination jurisdiction is deemed by Superintendency to offer appropriate levels of protection	Yes	Fine of up to 2,000 times Colombia's minimum wage; suspension of the database for up to six months	
Ecuador*	In July, Ecuador's President, Gabriela Rivadeneira, presented a bill on the protection of privacy and personal data. The bill requires organizations that collect and use personal data to obtain prior consent from data subjects. It also prohibits data transfers to countries or international organizations that do not provide adequate levels of data protection according to international or regional standards. To oversee compliance, the bill also seeks to create a National Authority for Personal Data Protection and requires organizations to register their databases on a national register managed by the new authority.			Yes, it includes provisions for access, rectification and erasure.	Penalties for non-compliance include fines, temporary suspension of databases or permanent closures.	Article explaining the bill: https://app.dataguidance.com/dataguidance_privacy_this_week.asp?id=7253
EU Proposed Data Protection Regulation	"Any information relating to a data subject." A data subject is "an identified natural person or a natural person who can be identified, directly or indirectly, by means	Yes, and "right to be forgotten" creates right to revoke consent at any time.	Yes, if approved by the Article 29 Working Party. New safe harbor agreements will have to be negotiated with the US and other foreign nations.	Yes	Private rights of action, civil and criminal penalties, to be determined by member states.	Current draft: http://ec.europa.eu/home-affairs/doc_centre/police/docs/com_2012_10_en.pdf

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
	reasonably likely to be used by the controller or by any other natural or legal person."					
EU Data Protection Directive Directive 95/46/EC ("EU DPD")	"Any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."	Yes, unless necessary for: (1) entering into or performing contracts; (2) protecting the vital interests of the subject; (3) carrying out the public interest or in the exercise of official authority; (4) the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed.	Yes, if considered to have adequate data protection standard approved by the Article 29 Working Party, which administers safe harbors such as the US-EU Safe Harbor.	Yes	Member states must provide private right of action and may impose civil or criminal sanctions.	
EU*	In July, the European Commission announced it finalized approval of a new and improved EU-U.S. Privacy Shield, replacing the previous iteration, which was struck down in October 2015. The U.S. Department of Commerce began accepting applications for self-certification under the new version on Aug. 1. The new Privacy Shield imposes stronger compliance obligations on U.S. companies, as well as stricter monitoring and enforcement requirements on the U.S. government. Some notable changes include a new Notice requirement that includes 11 new items that must be clearly disclosed to individuals when they are first asked to provide personal information, including information about the Privacy Shield, their right to access their personal data and that their data may be disclosed to public authorities. It also establishes new dispute			Yes, a right to access is included.	Yes, and Privacy Shield firms remain liable if a third-party partner processes personal information in conflict with the principles of the Privacy Shield.	Press release: http://europa.eu/rapid/press-release_IP-16-2461_en.htm

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	resolution mechanisms and stipulates that if an individual cannot settle a complaint with the company in question, it can access (at no charge) alternative dispute resolution solutions. Companies must also re-certify their compliance with the new Privacy Shield on an annual basis, and in the event they fall out of compliance, they now must return or delete all relevant data. It also contains stricter rules concerning third-party disclosure of data, stipulating that unless a company can prove it is not responsible, it remains liable if a third-party partner processes personal information in conflict with the principles of the Privacy Shield.					
EU*	The EU moves closer to extending telecom privacy rules to over-the-top (OTT) service providers. The EU appears ready to begin regulating OTT services (such as those providing instant messaging, voice-over-IP and email applications) using the same rules it applies to traditional telecommunications carriers. Currently, the ePrivacy Directive requires traditional telecom firms to protect users' security and prevents them from storing customer location and traffic data, but it doesn't extend those same restrictions to OTT providers.					Summary of findings: https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive
France Data Processing, Data Files and Individual Liberties Act	"Personal Data" means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him or her. "Sensitive Data" means Personal Data directly or indirectly relating to racial or ethnic origins, political opinions, trade union	Generally, informed, specific, and unambiguous consent is required (in French) to process personal data; sensitive data requires express, written consent or one of the above exception. EU DPD exceptions apply.	Yes, same as EU DPD Recommended to use an unmodified version of the model contractual clauses approved by the EC (2001, 2003, 2004, or 2010 models); alternatively, BCRs may be accepted to secure transfers of data outside the EU (i.e. internal rules applicable to data exporter and data importer).	Yes	Civil/criminal penalties; maximum fine of €1,500,000 for companies, individuals can face a maximum fine of €300,000 and 5 years of imprisonment; private right of action for damages.	

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	membership, religious or philosophical beliefs, health or sexual life.					
France*	The French Data Protection Authority (CNIL) published the results of the Internet sweep on connected devices. The sweep was conducted in May 2016 to assess the quality of the information provided to users of connected devices, the level of security of the data flows and the degree of user empowerment (e.g., user's consent and ability to exercise data protection rights). The CNIL's two main findings were: 1) users of connected devices are not sufficiently informed of the processing of their personal data and 2) users have a satisfactory degree of control over their personal data.					Results of the sweep: https://www.cnil.fr/fr/sweep-day-2016-des-objets-connectes-encore-trop-peu-transparents-sur-lutilisation-des-donnees
Germany Federal Data Protection Act Amendments	N/A	As of September 1, 2012 all marketing or advertising that uses personal data will require express opt-in consent. This needs to be specifically brought to the attention of data subjects as part of a terms and conditions governing their data with the data collector.	N/A	Yes, data subjects may object to the use or transfer of their data and must be informed if advertisement about their right to object	This comes at the end of a 3-year grace period following the amendments to Germany's Federal Data Protection Act in 2009. Exemptions are still applicable for when data collecting companies use personal data for their own offers or when third-party advertisers without consent of data subjects clearly indicate the source of personal data.	http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
Germany Federal Data Protection Act	"Personal Data" means any information relating to personal or material circumstances of an identified or identifiable individual; "Sensitive Personal Data" means any information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life.	Consent must be voluntary, informed, and give in writing (handwritten signature or by a qualified e-signature, unless other form allowed); notice to be given in German language or any other that data subject has a sufficient proficiency in. German courts require that declarations of consent that are given simultaneous to other declarations in standard form agreements must include a separate clause and signature line for data collection. EU DPD exceptions apply. "Informed" means that data subject is given the following information prior to any collection: (i) the identity of the data controller; (ii) purposes of	Yes, same as EU DPD	Yes	Civil/criminal penalties; max. administrative fine for repeated violations was €1.46M; private right of action.	

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
		collection; (iii) intended recipients or categories of recipients and their location; (iv) categories of data involved; (v) any information relevant for the data subject to decide whether to consent; and (vi) insofar as possible, the consequences of the data subject withholding consent. Note: Informed consent may NOT be implied from the data subject's actions or inaction.				
Germany*	The DPA for the German state of North Rhine-Westphalia became the first to publish its guidelines. Specifically, the DPA introduced a requirement for German companies to conduct due diligence on Privacy Shield-certified U.S. companies prior to permitting a transfer of EU data to them. This includes evaluating the U.S. company's privacy notice and monitoring its onward transfer compliance (for ensuring third parties comply with the Privacy Shield principles). In addition, much like the new Privacy Shield requires compliant organizations looking to transfer data to a processor to have a written contract in place governing the processing relationship, German countries that transfer data to U.S. processors – even those certified as Privacy Shield-compliant – must also conclude a separate data processing contract.					The guidelines (in German): http://www.alstonprivacy.com/wp-content/uploads/2016/09/NRW-Privacy-Shield-FAQs.pdf.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
Ghana Data Protection Act (Act. 843)	Any data about an individual who can be identified, (a) from the data, or (b) from the data or other information which is in the possession of, or is likely to come into the possession of the data controller, and among others comprises (i) an expression of opinion about the individual, and (ii) an indication of the intentions of the data controller	Requires either the (i) prior consent of the data subject, or (ii) when one of the following conditions is met: (a) for the purpose of a contract to which the data subject is a party; (b) is authorized by law; (c) to protect a legitimate interest of the data subject; (d) for the proper performance of a public law duty; or (e) when necessary to pursue the legitimate interest of the responsible party or a third party to whom the data is supplied.	Yes	Yes	Data Protection Commission can enforce civil/criminal penalties, max. two years of imprisonment.	http://www.parliament.gh/assets/file/Bills/Data%20Protection%20Act,%202010.pdf Note: Implementing regulations still need to be passed
Hong Kong Personal Data Privacy Ordinance ("PDPO")	Any data relating directly or indirectly to a living individual and from which it is practicable to ascertain the identity of an individual and which is in a form in which access to or processing of the data is practicable.	Not generally required as long as the data user tells the data subject at the time of or before collection the purpose for which the data is to be used and the classes of persons to whom the data may be transferred. Data	Only if the data user has reasonable grounds to believe the destination jurisdiction has substantially similar provisions to the HK ordinance; if the data subject consents in writing; or the data user has exercised due diligence to	Yes	Civil/criminal penalties, private right of action for damages.	

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
		may not be used for direct marketing purposes unless the data subject is provided with the option to opt-out.	ensure the Personal Data will not be treated in a manner that will contravene the ordinance.			
Hong Kong*	The Privacy Commissioner for Personal Data (PCPD) Hong Kong issued an "information leaflet" detailing BYOD best practices and guidelines, and emphasized the fact that organizations permitting BYOD remain fully responsible for complying with the country's Personal Data (Privacy) Ordinance and its Data Protection Principles.					Full text: https://www.pcpd.org.hk/english/resources_centre/publications/files/BYOD_e.pdf
India Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules ("Privacy Rules")	Any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person; "Sensitive Information" relates to: (i) password; (ii) financial information e.g., bank account/credit or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v)	Unclear, except processing sensitive information requires written, explicit consent including notice of the purpose of collection and use.	Yes, as long as the transborder data flows of sensitive personal data are made to another entity or country with the same level of data protection as adhered to in India, and that the transfer is required for a contractual purpose.	Yes, however, procedures have not been adopted for data subjects to review information.	Unclear	http://deity.gov.in/content/information-technology-act

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
	medical records and history; and (vi) biometric information.					
India Privacy Bill 2014	Any data which relates to a data subject, if that data subject can be identified from that data, either directly or indirectly, in conjunction with other data that the data controller has or is likely to have and includes any expression of opinion about such data subject.	Yes, consent is required for disclosure.	Yes, provided that such country has sufficient data protection standards and detailed notice of such transfer is provided.	Yes.	Offenses may include criminal penalties. Includes penalties for: -obtaining data under false pretenses -unauthorized collection, use, or disclosure of personal information -contravention of regulatory authority Civil right of action can be brought if loss or damage has been suffered or an adverse determination is made about an individual due to negligence on complying with the law.	Currently in draft form by the Department of Personnel and Training, Government of India: http://www.medianama.com/2014/04/223-leaked-privacy-bill-2014-vs-2011-cis-india/
Indonesia Law No. 11 of 2008 on Electronic Information and Transactions ("EIT Law")	Data of individuals which must be stored and maintained without error and the secrecy of which is protected.	Data subjects must give consent to use of any personal information. No specification as to whether that is opt-in or opt-out. (Article 26)	Yes, as long as done with the data subject's consent or some other means of authorization.	No	Individuals may "lodge a claim for damages under the law" (Article 26(2))	

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
Ireland Data Protection (Amendment) Act	"Personal Data" means data relating to a living individual who is or can be identified from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. "Sensitive Personal Data" means: (i) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject, (ii) whether the data subject is a member of a trade union,(iii) the physical or mental health or condition or sexual life of the data subject, (iv) the commission or alleged commission of any offence by the data subject, or (v) any proceedings for an offence committed or alleged to have been	Yes, explicit and obtained prior to processing. EU DPD exceptions apply.	Yes, same as EU DPD.	Yes	Private rights of action, civil and criminal penalties, max. €5,000 for fines and max. €	

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.					
Ireland*	Ireland's Data Protection Commissioner's office issued detailed guidance aimed at helping individuals better understand how information on their location is collected and processed, as well as to clarify all organizations' obligations regarding location data.					The text of the guidance: https://www.dataprotection.ie/docs/09-08-2016-Data-Protection-Office-issues-Guidance-on-Location-Data/1588.htm
Israel The Protection of Privacy Law	Details concerning an individual's personality, personal status, intimate relations, health condition, financial condition, vocational qualifications, opinions and religious belief.	Yes, informed consent, express or implied	Yes, requires that the receiving country ensures a level of protection of personal information that equals or exceeds the level of protection provided under Israeli law.	Yes, including objection to direct marketing, and deletion.	Strict criminal liability up to one year imprisonment; or civil tort fines that accumulate daily between ~$70,000, up to max. of $1,000,000.	
Israel*	New draft guidelines issued by the Israel Law, Information and Technology Authority (ILITA) specifies that surveillance cameras installed in the workplace for security reasons cannot be used to monitor employees. For example, if surveillance video is reviewed out of concern that a stranger entered the premises, and a worker is seen in the background taking an unauthorized break, that footage can't be used against the worker. The guidance also states, however, that in addition to security, surveillance cameras can be used by managers to oversee employees, for example, to monitor the quality of service they provide customers.					The full guidance (in Hebrew): http://www.justice.gov.il/Units/ilita/MainDocs/%D7%98%D7%99%D7%95%D7%98%D7%AA%20%D7%94%D7%A0%D7%97%D7%99%D7%99%D7%AA%20%D7%9E%D7%A6%D7%9C%D7%

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	In those cases, however, cameras can be installed only after the employer has formulated a clear policy and communicated that policy to employees.					9E%D7%95%D7%AA%20%D7%91%D7%A2%D7%91%D7%95%D7%93%D7%94%20-%2028-8-16.pdf
Italy Data Protection Code	"Personal Data" means any information concerning natural persons that are or can be identified also by way of other items of information – e.g., via a number or an ID code; "Sensitive Data" means any data that can disclose a person's racial origin or ethnicity, religious or other beliefs, political opinions, membership of parties, trade unions and/or associations, health, or sex life.	Consent must be express (not implied), free, specific (for each data processing purpose sought by the Data Controller); given prior to the commission of processing; and documented in writing (albeit, may be given orally, but requires a report on paper medium). Consent is not always mandatory because the Code provides for specific exemptions (e.g., processing that is necessary to perform contractual obligations, to comply with specific requests made by the data subject prior to entering into a contract, or to comply with laws and regulations). However, processing sensitive data would	Yes, same as EU DPD	Yes	Private right of action; Civil/criminal penalties of up to two years imprisonment, max. €120,000 administrative fines.	

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
		require express, written consent or one of limited exceptions. EU DPD exceptions apply.				
Japan Act on the Protection of Personal Information	Any information that would make a living individual distinguishable from others.	Business handling personal information must specify the "purpose of utilization" at the time of collection and can't change the purpose beyond the scope without obtaining consent from data subject. Can't share with a third party without obtaining prior consent of data subject. (Note: "third party" not defined, but affiliates are assumed to be third parties.)	Notice not required.	Yes	"Competent minister" may order business to take measures to come into compliance with statute.	
Macau Personal Data Protection Act	"Personal data" defined as information of any type relating to an identified or identifiable natural person, defined as one who can be identified, directly or indirectly, in	Opt-in consent not required - opt-out consent OK as long as data subject gets privacy notice and opportunity to opt out of use of info for marketing. Need prior authorization from authorities	Notice/consent (opt-out ok) required.	Yes	Various	

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	particular by reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.	before processing "personal data relating to credit and solvency of the data subjects."				
Malaysia Personal Data Protection Act	"Personal data" defined as data in electronic form which relate to a living person who can be identified (a) from those data, or (b) from those data and other information which is in the possession of the organization. "Sensitive personal data" includes data on physical or mental health condition, political opinions, religious beliefs, or criminal record.	Opt-out consent ok, but must get consent for use other than purpose for which data was collected (e.g., performance of a contract to which data subject is a party). Notice must be written, state purposes for which it is being collected/processed, right of access, choices regarding use of the data, and to whom the data will be disclosed.	Notice/consent required unless destination jurisdiction is deemed by Ministry of Information to offer adequate protection.	Yes	Data users who fail to comply with the code of practice are liable for fines NTE 100,000 ringgit or prison term NTE 1 year or both.	
Mexico Data Protection Law	"Personal data" defined as any information that refers to an identified or identifiable individual.	Opt-out consent ok. Implied consent is acceptable in emergencies or for compliance with contracts to which subject and data controller are parties.	Notice/consent only required if transfer is not for the purpose for which the data was originally collected.	Yes	Up to $1.5M ($3M for sensitive personal data); up to 5 years imprisonment (10 years for sensitive personal data).	

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
Peru Reglamento de la Ley No 29733, Ley de Protección de Datos Personales ("Regulations")	"Personal data" defined as any information on an individual, which identifies or makes him/her identifiable through means that may be reasonably used.	Prior, informed, express and unequivocal consent required unless "necessary to perform a contract to which the data subject is a party."	Written consent required for transfers to countries where rights to protection of data are deemed inadequate.	Yes	Up to 10% of the violator's annual gross income	
Philippines Data Privacy Act of 2012	Any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.	No, but freely-given, specific, informed consent is needed in certain circumstances, as with sensitive categories of data.	Unclear - Regulations and rules still being adopted, but data controller is responsible for the data's proper transfer and protection in receiving country.	Yes	Penalties of imprisonment ranging from 1.5 years to 5 years and a fine of min. Php500,000 and max. Php 1,000,000.	http://www.gov.ph/2012/08/15/republic-act-no-10173/; Note, implementing regulations still need to be issued
Philippines DTI Guidelines (Voluntary)	"Personal data" defined as any information relating to an identified or identifiable natural person.	Consent required for initial collection and for any use besides that for which initially collected.	Notice/consent not required.	Yes	None	

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
Philippines*	The National Privacy Commission of the Philippines released the final text of its Implementing Rules and Regulations (IRR) for the Data Privacy Act of 2012. The draft IRR, released in June, stipulated that the processing of personal data must adhere to the principles of transparency, legitimate purpose and proportionality. It defined personal data as personal information, sensitive information and privileged information, and stated that any personal information controller must take organizational, physical and technical security measures to ensure data protection. It also stipulated that data subjects must give consent prior to any data collection, and that data subjects must be notified within 24 hours once an organization realizes a security breach affecting their data has occurred. The final IRR clarifies several points, including the difference between "personal data" and "personal information," rules for data collected in foreign jurisdictions but processed within the Philippines, specific data breach notification requirements and more.					Full text: https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/09/20160825-IRR-RA-10173-data-privacy.pdf
Romania Law No. 677/2001 Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data	Personal data is defined as "any information referring to an identified or identifiable person; an identifiable person is a person that can be identified, directly or indirectly, particularly with reference to an identification number or to one or more specific factors of his physical, physiological, psychological, economic, cultural or	Yes. Processing of personal data can only be carried out if the data subject has given his/her express and unequivocal consent.	Yes, "only if the Romanian law is not infringed and the state of destination ensures an adequate level of protection."	Yes. Every data subject has the right to obtain from the data controller, upon request, and free of charge, once a year, confirmation of the fact that the data concerning him/her are or are not being processed by the data controller. Every data subject has the right to obtain from the data controller, upon request, and free of any charge rectification,	The National Supervisory Authority for Personal Data Processing has investigatory powers, can order suspension of processing and other sanctions, and may bring suit in court on behalf of individuals. Minor offenses are liable for a fine of 5 million to 500 million ROL.	http://ec.europa.eu/justice/policies/privacy/docs/implementation/ro_law_677_2001_en_unofficial.pdf

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
	social identity."			updating, blocking or deletion of data whose processing does not comply with the provisions of the present law, notably of incomplete or inaccurate data.		
Russia Law No. 152-FZ On Personal Data ("OPD Law")	"Personal data" defined as any data relating to a directly or indirectly identified or identifiable individual.	Consent required and may be revoked by subject at any time. Written consent required for collection of sensitive information.	Written consent required for transfers to countries where rights to protection of data are deemed inadequate.	Yes	Private rights of action, civil and criminal penalties.	
Singapore Personal Data Protection Act ("PDPA")	"Personal Data" means data, whether or not true, about an individual who can be identified from that data, or identified from that data and other information to which the organization is likely to have access; excludes business contact information, including work email/phone number and titles.	Yes, consent must be obtained from the data subject before the collection, use and disclosure. Consent can either be (i) *actual* (i.e. informed how a reasonable person would consider appropriate in the circumstances); or (ii) *deemed* (i.e. where the individual voluntarily gives personal data for a reasonable purpose).	Yes, organizations can transfer data to recipients in third countries as long as they ensure a comparable standard of protection for the personal data (e.g., through contractual arrangements). Additionally, organizations can seek exemptions.	Yes	The Personal Data Protection Commissioner (PDPC) can direct organizations to pay penalties of up to SGD1M; additionally a person may be punished by imprisonment. The PDPA recognizes a right of private action and holds employers jointly liable for employees' violations.	All provisions of the PDPC are now in effect. https://www.pdpc.gov.sg/personal-data-protection-act/overview.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
***Singapore**	On April 21, the Personal Data Protection Commission of Singapore released its "Advisory Guidelines on Enforcement of the Data Protection Provisions Issued by the Personal Data Protection Commission." The guidelines, which are only advisory in nature and not legally binding on the commission or anyone else, are designed to provide insight into how the commission will interpret the PDPA's provisions relating to data protection.					https://www.pdpc.gov.sg/docs/default-source/advisory-guidelines-on-enforcement/advisory-guidelines-on-enforcement-of-dp-provisions-(210416).pdf?sfvrsn=2
South Africa Protection of Personal Information Bill	Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person	Voluntary, specific and informed expression of will in terms of which a data subject agrees to processing of personal information relating to him or her required unless: processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party; processing complies with an obligation imposed by law on the responsible party; processing protects a legitimate interest of the data subject; processing is necessary for the proper performance of a public law duty	Yes, if: the recipient of the information is subject to a law, binding code of conduct or contract which imposes standards substantially similar to POPI; the data subject consents; the transfer is necessary for performance of a contract between the data subject and the responsible party; the transfer is necessary for performance of a contract 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 it is not	Yes	Civil cause of action, fines, or imprisonment	Signed by president and enacted. http://www.info.gov.za/view/DownloadFileAction?id=105938

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
		by a public body; or processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.	reasonably practicable to obtain the consent of the data subject and if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.			
South Korea Personal Information Protection Act ("PIPA")	"Personal Information" defined as information concerning anyone living ...which allows for the possibility for the individual to be identified by name and resident registration number.	Must give notice with specified info. Subject must be able to opt-out of collection and/or use of data.	Yes, requires data subject's consent.	Yes	Penalties for negligence – fines up to max. 5M won.	
South Korea	South Korea updated its PIPA and IT Network Act, reflecting the country's continuing emphasis on privacy and data protection issues. Amendments to PIPA include stipulations that: • Residence registration numbers (RRNs) must always be encrypted and can only be processed without consent in cases expressly authorized by law. • New technical, organizational and physical measures be implemented to protect sensitive information. • Data subjects be notified when their data is transferred to third parties, including information about the organization receiving the data and the purpose of the transfer. • Increased fines (up to KRW 3 million) for data breaches, with those affected no longer having to prove actual damages.					https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/05/bkl-Legalupdate-20160426_v2.pdf

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
Spain Royal Decree 1720/2007	"Personal Data" means any alphanumeric, graphic, photographic, acoustic or any other type of information relating to an identified or identifiable individual. "Sensitive Data" means information relating to ideology, religion, beliefs, racial, origin, health or sexual life, trade union membership, and criminal or administrative offenses.	Processing personal data, generally, requires obtaining the data subject's free, prior, unequivocal consent, which can be express (e.g., written) or tacit (as long as there is a prior notice of 30 working days), and where the data subject understands which information is being collected (i.e. informed).	Same as EU DPD.	Yes	Violations subject to penalties ranging from €900 to €600,000 depending on factors, including the nature of the personal rights affected, the volume of data concerned, the profits obtained, intent, and the continued nature of the infringement, etc.; private rights of action	
Sweden Swedish Personal Data Act	"Personal Data" means any information relating to an identified or identifiable natural, living person. "Sensitive Data" means Personal Data relating to race, ethnic origin, political opinions, health or sex life, religious or philosophical beliefs, and membership to a trade union.	Consent may be express, though not necessarily in writing, or tacit. Notice for consent should be in Swedish or in a language known to data subject.	Yes, same as EU DPD.	Yes	Private rights of action, civil and criminal penalties.	

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
Switzerland Federal Ordinance on the Federal Law on Data Protection ("FLDP")	All information relating to an identified or identifiable person. "Sensitive Personal Data" includes religious, ideological, political or trade union-related views or activities, health, the intimate sphere, racial origin, social security measures, administrative or criminal proceedings; IP addresses may qualify as well	Requires at least informed, voluntary consent in advance to processing; implicit consent is insufficient for sensitive personal data	Yes, only if transferee is in a country with legislation providing an adequate level of protection; Note: U.S.-Swiss "Safe Harbor" framework is same as of E.U.-U.S. Safe Harbor.	Yes	Private rights of action, civil and criminal penalties; fines up to max. CHF 10,000, with more severe criminal sanctions for breaches of professional secrecy.	
Taiwan Personal Data Protection Act ("PDPA")	"Personal information" defined as name, DOB, ID card number, passport number, characteristics, ...financial conditions, contact information, social activities, and other information which may be used to identify a natural person.	Must give notice with specified information and obtain "written consent" to collection and use of data. Use may be on opt-out.	Yes, but may be restricted in 4 cases: (i) where it involves major national interests; (ii) it involves a treaty, (iii) the country receiving the data lacks adequate data protection that might harm the data subjects' interests; or (iv) the transfer abroad is made to evade the PDPA.	Yes	Private rights of action, civil and criminal penalties, with fines max. of NT$200,000.	
Turkey No Comprehensive Statute						

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
Ukraine Law No. 2297-VI On the Protection of Personal Data	Information on natural persons, who are identified or identifiable; treated as "information with restricted access"	Yes in writing, except when protection of vital interests of data subject are involved and cannot be obtain consent	Yes, if transferee ensures the protection, and obtains any respective consent	Yes, including the location of the databases containing their data, the conditions of access to the database, and any third party recipients	Max civil fines of EUR 1,7000 per violation; Data subjects have a right to compensation for damage, including moral or emotional distress	
United Arab Emirates Dubai International Financial Centre (DIFC) only DIFC Data Protection Law	Information relating to an identifiable natural person, i.e. who can be identified, directly or indirectly, in a particular by reference to an identification number or to one or more factors specific to his biological, physical, biometric, physiological, mental, economic, cultural or social identity; "sensitive data" reveals or concerns racial or ethnic origin, communal original, political affiliations or opinions, religious or philosophical beliefs.	Yes	Yes to entities or countries listed as acceptable jurisdiction; or can seek written approval of the Commissioner where there is an adequate level of protection in the transferee-country.	Yes, with rights to the rectification, erasure, or blocking of non-compliant data	Max. fine of $25,000 for failure to register with Commissioner, $20,000 for transferring outside DIFC without permit, $10,000 for processing personal data without permit; $15,000 for disallowed processing	

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
United Kingdom Cookie Tracking Law (implementing the EU e-Privacy Directive)	No change (same as under existing privacy laws; see http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx).	Companies must provide notice and obtain consent for any cookies that collect personal data. Implied consent is OK if users understand that their actions will result in cookies being set.	N/A	N/A	As the regulation is phased in, monetary penalties will only be levied when a violation cases substantial harm and is willful.	The law just took effect. Guidance provided by the UK Information Commissioner's Office (ICO): http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx
United Kingdom Data Protection Act ("DPA")	"Personal Data" means data related to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller. Includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. "Sensitive Personal Data" means Personal Data consisting of	Consent can be express (not necessarily in writing) or implied, but must: (i) signify the data subject's agreement with some active communication between the parties; and (ii) must be an adequate consent appropriate under the circumstances.	Same as EU DPD.	Yes	Private rights of action, civil and criminal penalties, with max. fines of £500,000 for serious breaches of the DPA's principles.	

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	information as to (a) the racial or ethnic origin of the data subject, (b) political opinions, (c) religious beliefs or other beliefs of a similar nature, (d) membership to a trade union; (e) physical or mental health or condition, (f) sexual life; (g) (alleged) commission of an offence, or (h) any proceedings for any offense committed, the disposal of such proceedings or the sentence of any court in such proceedings.					
Uruguay	Regulations require public agencies store data on servers within the country's boundaries. The regulations also ban the use of non-government websites or e-mail accounts by government agencies and by public officials conducting formal duties and require that all government e-mail be encrypted.					http://archivo.presidencia.gub.uy/sci/decretos/2014/04/cons_min_827.pdf (local language)

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
Zimbabwe	The government announced that it is in the process of developing new cyber laws to regulate social media. Bills are ready to be brought to the attorney general for final drafting. After the final draft is complete they will be brought to the Cabinet and then to Parliament.					http://jurist.org/paperchase/2014/08/zimbabwe-drafting-cyber-laws-to-regulate-social-media.php