International Privacy Laws and Related Developments – Q2 2016
(* indicates update from Q1 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.	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	Yes, but the transferring organization must ensure that the receiving organization overseas does not breach the APPs. Note- the transferring	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-

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
	The definition of "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.	the information to be used for. Where consent is required it can be either express or implied.	organization is liable for any breach of the recipient.			factsheet17_Australian_privacy_principles.pdf
Australia Privacy Amendment (Privacy Alerts) Bill 2014	"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	N/A	N/A	N/A	Civil penalties of up to $1.7 million for corporate violations.	Currently before the Australian Senate. http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s958

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	b. whether the information or opinion is recorded in a material form or not." Companies must notify affected individuals in the event it reasonably believes that a security breach has occurred that may result in "risk of serious harm" to the individuals to whom the information relates. In the event of breaches related to personal information, credit reporting information, credit eligibility information, or tax file number information, companies must also prepare a statement notifying the Commissioner, providing a copy of consumer notices, and describing the nature of the breach.					

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
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 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	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) 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.	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) 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	Yes	Complaint process through Commissioner; fines range from AUD10,000 to AUD40,000.	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	personal information; (B) health information about an individual; or (C) genetic information about an individual that is not otherwise health information.		consent; or (F) transferor has taken reasonable steps to ensure info is used by transferee consistent with the NPPs.			
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). http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
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. If a breach could be reasonably believed to create a real risk of significant harm to an individual, it must be disclosed to the	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

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
	Commissioner in a report detailing the nature of the breach.					
***Canada** Amendments to Saskatchewan's HIPA privacy legislation	New amendments to the government of Saskatchewan's HIPA privacy legislation are designed to increase the accountability of trustees and employees of trustees responsible for protecting private health information. In addition, the changes also establish a process for responding to discovery of abandoned or unsecured records.					The amendments went into effect June 1, 2016/ https://www.saskatchewan.ca/government/news-and-media/2016/may/31/hipa
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

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

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, identification 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	
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	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
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 reasonably likely to be used by the controller or by any other natural or legal person."	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
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.	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
***EU**	The European Parliament approved the EU GDPR, which now officially replaces the old EU data protection rules (which dated back to 1995). The rules include a: • Right to be forgotten. • Requirement for obtaining clear consent for processing private data by the person concerned. • Right of individuals to transfer their personal data to another service provider. • Right of individuals to know when their data has been hacked. • Requirement for processors to post clear and understandable privacy policies. • A directive on data transfers for policing and judicial purposes, setting minimum standards within each member state to make it easier for member states to exchange and share data for law enforcement.				Yes, including fines up to 4 percent of firms' total worldwide annual revenue.	The new GDPR was published in the EU Official Journal on May 4 and entered force on May 24, although it will not be directly applicable to all EU member states until May 25, 2018./http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm
***EU**	On April 14, the EU parliament approved the PNR bill, which regulates the use of passenger name record data in the EU for the prevention, detection, investigation and prosecution of terrorist offenses and serious crimes. The new law obliges airlines to hand over passenger data to national authorities for all flights from non-EU countries to the EU and vice versa. The PNR data must be retained by the airlines for five years, but after six months, the data must be stripped of anything that may be used to identify individuals.					The new regulation was published in the EU Official Journal on May 5, and member states have until May 6, 2018, to transpose it into their national laws/ http://www.europarl.europa.eu/news/en/news-room/20150123BKG12902/EU-Passenger-Name-Record-(PNR)-directive-an-overview

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
***EU**	On May 17, the EU Council adopted the EU Network and Information Security (NIS) The NIS aims to provide an EU-wide strategy for dealing with cyber threats. It covers the handling of attacks on digital systems and requires organizations that suffer cyberattacks to notify authorities in the member states where they are based. The directive applies to companies within critical sectors (banking, health care, energy and transport) and requires them to notify national authorities of any cyberattack that has "a significant impact on the continuity of the essential services they provide." It also requires service providers to notify the authorities whenever they experience "a substantial impact on the provision of a service" offered within the EU.					It is expected to enter force in August, although member states have a 21-month period to adopt the provisions, meaning it won't likely take effect until May 2018/ http://www.consilium.europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/
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 membership, religious or philosophical beliefs, health or sexual life.	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.	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

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 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
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	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	Yes, same as EU DPD	Yes	Civil/criminal penalties; max. administrative fine for repeated violations was €1.46M; private right of action.	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	or sex life.	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 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				

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
		data subject's actions or inaction.				
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	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	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	Yes	Civil/criminal penalties, private right of action for damages.	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	processing of the data is practicable.	persons to whom the data may be transferred. Data may not be used for direct marketing purposes unless the data subject is provided with the option to opt-out.	writing; or the data user has exercised due diligence to ensure the Personal Data will not be treated in a manner that will contravene the ordinance.			
Hong Kong	The Privacy Commissioner for Personal Data published guidance, titled, "Data Breach Handling and the Giving of Breach Notifications," to provide businesses with steps to resolve a data breach.					http://www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_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	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

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
	condition; (iv) sexual orientation; (v) 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. 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 was suffered or adverse determination is made about an individual due to negligence on compliance.	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))	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

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. €	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

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.					
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.	
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,	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	Yes, same as EU DPD	Yes	Private right of action; Civil/criminal penalties of up to two years imprisonment, max. €120,000 administrative fines.	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
	health, or sex life.	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 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	Notice not required.	Yes	"Competent minister" may order business to take measures to come into compliance with statute.	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
		assumed to be third parties.)				
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 particular by reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.	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 before processing "personal data relating to credit and solvency of the data subjects."	Notice/consent (opt-out ok) required.	Yes	Various	
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.	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	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.	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	"Sensitive personal data" includes data relating to physical or mental health condition, political opinions, religious beliefs, or criminal record.	collected/processed, right of access, choices regarding use of the data, and to whom the data will be disclosed.				
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	Monetary penalties of up to $1.5M ($3 M for sensitive personal data); criminal penalties of up to 5 years imprisonment (10 years for sensitive personal data).	
***Norway**	In April 2016, the Norwegian Data Protection Authority (DPA) said it will begin requiring companies to notify individuals when their personal data is disclosed without their consent. Prior to this, Norwegian laws did not specify a general right for individuals to be informed of data breaches. The country's Personal Data Regulation did require that any data controller who discovers a breach of confidential personal information notify the DPA, and the Personal Data Act stipulated that data subjects be provided with information concerning possible disclosures of personal information, as well as the identity of the recipient. Neither provision alone, however, guaranteed individuals a clear right to be informed when their personal data was disclosed to unauthorized parties.					https://www.datatilsynet.no/Nyheter/2016/ma-si-fra-til-berorte2/ (in Norwegian)
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	Prior, informed, express and unequivocal consent required unless "necessary to perform a contract to which the data	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	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
	may be reasonably used.	subject is a party."				
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	
Romania Law No. 677/2001 Protection of Individuals with Regard to the Processing of Personal Data and	Personal data is defined as "any information referring to an identified or identifiable person; an identifiable person is a person that can be	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	The National Supervisory Authority for Personal Data Processing has investigatory powers, can order suspension of processing and	http://ec.europa.eu/justice/policies/privacy/docs/implementation/ro_law_677_2001_en_unofficial.pdf

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
the Free Movement of Such Data	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 social identity."			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, updating, blocking or deletion of data whose processing does not comply with the provisions of the present law, notably of incomplete or inaccurate data.	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.	
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	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	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).	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	All provisions of the PDPC are now in effect. https://www.pdpc.gov.sg/personal-data-protection-act/overview.

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	likely to have access; excludes business contact information, including work email/phone number and titles.	appropriate in the circumstances); or (ii) *deemed* (i.e. where the individual voluntarily gives personal data for a reasonable purpose).	Additionally, organizations can seek exemptions.		PDPA recognizes a right of private action and holds employers jointly liable for employees' violations.	
***Singapore**	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.					Released April 21, 2016 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	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	Yes	Civil cause of action, fines, or imprisonment	Signed by president and enacted. http://www.info.gov.za/view/DownloadFileAction?id=105938

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
		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 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.	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 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.				Yes, increased fines (up to KRW 3 million) for data breaches, with those affected no longer having to prove actual	https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/05/bkl-Legalupdate-20160426_v2.pdf

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	• 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.				damages.	
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	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.	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
	opinions, health or sex life, religious or philosophical beliefs, and membership to a trade union.					
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	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	Yes	Private rights of action, civil and criminal penalties, with fines max. of NT$200,000.	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
	person.		abroad is made to evade the PDPA.			
***Turkey** Law on Personal Data Protection	Turkey's first data protection law shares many aspects of the EU's Data Protection Directive (95/46/EC), and seems to be Turkey's attempt to harmonize its data protection laws with those of the EU, which it is hoping to join. Like the EU directive, the Turkish law distinguishes personal data from sensitive data, and makes sensitive data subject to added protections. Like in the EU, sensitive data includes information such as racial and ethnic origin, political opinion, union membership and data about health and sex life, although Turkey also adds a data subject's personal appearance to that list. The new law also requires express consent before personal data may be processed and imposes restrictions on the transfer of personal data outside Turkey, stipulating that data subjects must give consent and receiving countries must offer sufficient data protection. The cross-border transfer rules do not go into effect until Oct. 7, 2016					Went into force April 7, 2016 / http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=6257
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	Yes	Yes to entities or countries listed as acceptable jurisdiction; or can seek written approval of the Commissioner where there is an adequate	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	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	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.		level of protection in the transferee-country.		data without permit; $15,000 for disallowed processing	
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 which relate to a living individual who can be identified (a) from those data, or (b) from those data and other information	Consent can be express (not necessarily in writing) or implied, but must: (i) signify the data subject's agreement with some active communication	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.	

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue Security / Compliance Issue					
	which is in the possession of, or is likely to come into the possession of, the data controller, and include 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 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	between the parties; and (ii) must be an adequate consent appropriate under the circumstances.				

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.

Country	"Personal information"	Consent required?	Transfer to other countries allowed?	Access/ correction requirements?	Penalties	Status / Source
	Security / Compliance Issue	Security / Compliance Issue				
	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)
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

© 2016-2017 IANS. All rights reserved. For more information, write to info@iansresearch.com.