Data Protection Laws of the Worlds (v. 2015)

Country	USA	UK	Germany	China
1. Definitions	Definition of personal data Varies widely by regulation. The FTC now considers information that can reasonably be used to contact or distinguish a person, including IP addresses and device identifiers, as personal data. However, very few U.S. federal or state privacy laws define “personal information” as including information that on its own does not actually identify a person. Definition of sensitive personal data Varies widely by sector and by type of statute. Generally personal health data, financial data, credit worthiness data, student data, personal information collected online from children under 13, and information that can be used to carry out identity theft or fraud are considered sensitive. For example, US state data security breach notice and state data security laws typically cover name plus government identification number, financial account or payment card number, and in some states health insurance medical and/or biometric data, and user name and password for an online account.	Definition of personal data ’Personal data’ is defined under the Act as data relating to living individuals who can be identified: > - from the data, or > - from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and 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. Definition of sensitive personal data ’Sensitive personal data’ means personal data consisting of information as to: > - the racial or ethnic origin of the data subject > - his political opinions > - his religious beliefs or other beliefs of a similar nature > - whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992) > - his physical or mental health or condition > - his sexual life > - the commission or alleged commission by him of any offence, or > - any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.	Definition of personal data The BDSG defines personal data as any information concerning the personal or material circumstances of an identified or identifiable natural person (‘data subject’). Definition of sensitive personal data Sensitive or rather special categories of personal data under the BDSG are any information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life.	Definition of personal data Under the Guideline, personal data refers to any data or information in connection with a specific individual, which can be used, separately or in combination with other data, to identify an individual. Personal data (which is referred to as ‘personal information’ in the Decision) means any electronic information which can enable you to identify a citizens individual identity and which relates to personal privacy. The Consumer Law does not provide a definition for personal data or personal information. Under the Draft Law, personal data (which is referred to as "personal information") means personal identity information such as the name, date of birth, ID card number, biometric data, occupation, address or telephone number, which are recorded electronically or in other means, and other information which individually or collectively may serve to identify a person. Definition of sensitive personal data The Guideline makes distinction between personal sensitive information and personal general information. Under the Guideline, sensitive personal data (which is referred to as ‘personal sensitive information’ in the Guideline) is defined as personal information the leakage or alteration of which may result in adverse impact to the data subject. What is the content of personal sensitive information would depend on the intention of the data subject and the specific characteristic of the business at hand. Examples may include personal identification number, cell phone number, race, political view, religious belief, genes or fingerprints. Personal general information is those other than personal sensitive information. Neither The Decision nor the Consumer Rights Law makes such distinction.

2. Authority	NATIONAL DATA PROTECTION AUTHORITY No official national authority. However, the FTC has jurisdiction over most commercial entities and has authority to issue and enforce privacy regulations in specific areas (eg for telemarketing, commercial email, and children's privacy). The FTC uses its general authority to prevent unfair and deceptive trade practices to bring enforcement actions against inadequate data security measures, and inadequately disclosed information collection, use and disclosure practices. State attorneys general typically have similar authority and bring some enforcement actions, particularly in the case of high profile data security breaches. In addition, a wide range of sector regulators, particularly those in the health care, financial services, communications, and insurance sectors, have authority to issue and enforce privacy regulations.	Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF T +0303 123 1113 (or +44 1625 545745 if calling from overseas) F 01625 524510 www.ico.org.uk	Eah individual German state has a Data Protection Authority which is responsible for the enforcement of data protection laws and competent for data controllers established in the relevant state.	There is no national data protection authority in the People's Republic of China ('PRC').
3. Registration	There is no requirement to register databases.	Data controllers who process personal data must inform the Information Commissioner so that their processing of personal data may be registered and made public in the register of data controllers, unless an exemption applies. The registration is made via a simple online form and the ICO allows data controllers to use standard form sector specific descriptions of their processing when registering. These description set out in very broad terms > - what data is being collected > - why the data will be processed > - the categories of data subject data is collected from, and > - whether the data will be transferred either within or outside the European Economic Area. However, data controllers can also provide their own specific description of the their processing or tailor the standard form sector specific descriptions if they wish.	Unlike most European data protection regimes, German data protection law does not require a registration of automated data processing. In addition, even though the BDSG provides for a notification, such notification is the exception rather than the rule. This follows from the fact that the notification requirement is waived if the data controller has appointed a data protection officer ('DPO'), which is mandatory for all companies of a certain size (the obligation applies if more than nine persons are regularly involved in the automated processing of personal data). Automated data processing operations with respect to sensitive data are subject to prior checking by the data controller's internal DPO.	The PRC does not maintain a registration of personal data controllers, personal data processing activities, or databases containing personal information.

4. Data Protection Officers	With the exception of entities regulated by HIPAA, there is no requirement to appoint a data protection officer, although appointment of a chief privacy officer and an IT security officer is a best practice among larger organisations and increasingly among mid sized ones. In addition, Massachusetts law requires an organization to appoint one or more employees to maintain its information security program. The law applies to organizations that own or license personal data on residents of Massachusetts, and thus reaches outside the state.	There is no requirement in the UK for organisations to appoint a data protection officer.	Data controllers that deploy more than nine persons with the automated processing of personal data are obliged to appoint a DPO. Such a DPO may either be an employee or an external consultant that has sufficient knowledge in the field of data protection. The DPO is neither required to be a citizen nor a resident of Germany, but shall have the necessary expertise in German data protection law as well as reliability. The DPO shall in particular monitor the proper use of data processing programs and take suitable steps to familiarise the persons employed in the processing of personal data with the provisions of data protection. As far as sensitive personal data is concerned, such personal data is subject to examination prior to the beginning of processing (prior checking) by the appointed DPO unless the data subject has consented. In case of doubt, the DPO shall liaise with the competent authorities. Any intentional or negligent infringement of the statutory obligation to appoint a DPO may result in fines up to EUR 50,000. However, the fine shall be higher than the economic advantage gained through the infringement. Therefore, depending on the individual case, the fine may eventually be higher than EUR 50,000.	There is no legal requirement in the PRC for organizations to appoint a data protection officer. The Guideline however recommends that a specific institution or personnel be appointed to be responsible for the internal management of personal data privacy (‘Data Controller’).

5. Collection & Processing	US privacy laws and self regulatory principles vary widely, but generally require pre collection notice and an opt out for use and disclosure of regulated personal information. Opt-in rules apply in special cases involving information that is considered sensitive under US law, such as for health information, use of credit reports, student data, personal information collected online from children under 13 (see below for the scope of this requirement), video viewing choices, precise geolocation data, and telecommunication usage information. The FTC interprets as a "deceptive trade practice" failing to obtain opt in consent if a company engages in materially different uses or discloses personal information not disclosed in the privacy policy under which personal information was collected. It has, for example, sued to prevent disclosure of personal data as aprt of serveral bankruptcy proceedings. States impose a wide range of specific requirements, particularly in the employee privacy area. For example, a significant number of states have enacted employee social media privacy laws, and, in 2014 and 2015, a disparate array of education privacy laws. The US also regulates marketing communications extensively, including telemarketing, text message marketing, fax marketing and email marketing (which is discussed below). The first three types of marketing are frequent targets of class action lawsuits for significant statutory damages.	Data controllers may collect and process personal data when any of the following conditions are met: > - the data subject consents > - the data controller needs to process the data to enter into or carry out a contract to which the data subject is a party > - the processing satisfies the data controller's legal obligation > - the processing protects the data controller's vital interests > - the processing is required by an enactment, the Crown or the government > - the processing is required to perform a public function in the public interest, or to administer justice, or > - the data controller has a legitimate reason for the processing, except if the processing would damage the data subject's rights, freedoms or other legitimate interests. Where sensitive personal data is processed, one of the above conditions must be met plus one of a further list of more stringent conditions. Whichever of the above conditions is relied upon, the data controller must provide the data subject with fair processing information. This includes the identity of the data controller, the purposes of processing and any other information needed under the circumstances to ensure that the processing is fair.	The collection, processing and use of personal data is only admissible if explicitly permitted by the BDSG or any other legal provision or if the data subject has explicitly consented in advance. In practice, Section 28 BDSG is the most applicable statutory provision permitting collection, processing and use of personal data. For example, Section 28 para. 1 no. 1–3 BDSG provide that the collection, processing or use of personal data as a means of fulfilling one's own business purposes shall be admissible if it is: > - necessary to create, perform or terminate a legal obligation or quasi legal obligation with the data subject > - necessary to safeguard legitimate interests of the controller and there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of processing or use, or > - the personal data is generally accessible or the controller would be allowed to publish them, unless the data subject has a clear and overriding interest. Sensitive personal data may only be processed if: > - it is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his or her consent > - the data involved has manifestly been made public, by the data subject > - it is necessary to assert, exercise or defend legal claims and there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of collection, processing or use, or > - it is necessary for the purposes of scientific research, where the scientific interest in carrying out the research project significantly outweighs the data subject's interest in ruling out the possibility of collection, processing and use and the purpose of the research cannot be achieved in any other way or would require a disproportionate effort. Processing of employee data for employment related purposes is subject to a separate provision (Sec. 32 BDSG) according to which the collection, processing and use of employee data is only permitted regarding decisions on the establishment, implementation and termination of the employment contract. Whichever of the above conditions is relied upon, upon the first collection of personal	Under the Guideline, a Data Controller should have a specific, clear and reasonable purpose when collecting personal information. Before a Data Controller collects and process personal data, they should notify the data subject of the following: > - the purpose of processing > - collection manner and methods, specific content collected and its retention period > - scope of use, including disclosure or the scope of provision to other organization or facilities of personal information collected > - measures protecting personal information > - the name, address and contact information of the Data Controller > - the risk of providing the request personal information > - the consequences of not providing the requested personal data > - channels for submitting complaints, and > - if personal information is to be transferred or entrusted with another organization or facility, notify the data subject including but not limited to the following: purpose of transfer or entrustment, specific content and scope of use of transfer or entrustment, and the name, address, contact method of the personal information receiver or trustee. Consent is required from the data subject before the personal information can be processed. Consent can be explicit or implicit. Implicit consent is sufficient for collection of personal general information. Explicit consent is required for collection of personal sensitive information. Where the data subject clearly objects, collection should be discontinued or the personal information should be destroyed. Furthermore, personal information should be collected on a minimally required basis in a direct manner that has been notified to the data subject. Indirect or hidden collection methods are prohibited. Also, collection from those with limited or no capacity for civil conduct (generally persons less than 16 years old) are prohibited unless consent is acquired from their legal guardians. In case of continued collection, the data subject shall be able to customize, adjust or shut down the function of personal information collection. The Data Controller should process personal data for the stated purpose and within the scope that the Data Controller has notified to the data subject. The Data Controller should take measures to keep

6. Transfer	No geographic transfer restrictions apply in the US, except with regard to storing some government information. The Commerce Clause of the U.S. Constitution likely bars US states from imposing data transfer restrictions and there are no other such restrictions in US national laws. Please note that following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU safe harbor regime is no longer regarded as a valid basis for transferring personal data to the US.	Data controllers may transfer personal data out of the European Economic Area if any of the following conditions are met: > - the data subject consents. > - the transfer is essential to a contract to which the data subject is party. > - the transfer is needed to carry out a contract between the data controller and a third party if the contract serves the data subject's interests. > - the transfer is legally required or essential to an important public interest. > - the transfer protects the data subject's vital interests, or > - the data is public. Transfers of personal data to jurisdictions outside of the European Economic Area are allowed if the jurisdiction provides 'adequate protection' for the security of the data, or if the transfer is covered by 'standard contractual clauses' approved by the European Commission, or subject to an organisation's Binding Corporate Rules. There is no requirement in the UK to notify the ICO of the use of the standard contractual clauses or to file these with the ICO. For transfer of data to the United States, compliance with the US/EU Safe Harbor principles can satisfy the requirements of the UK's transfer restrictions.* * Please note that following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU safe harbor regime is no longer regarded as a valid basis for transferring personal data to the US. This section of the Handbook will be updated in due course to reflect regulator actions in the wake of the decision. In the meantime, please refer to DLA Piper's Privacy Matters blog http://blogs.dlapiper.com/privacymatters/ for more information and insight into the decision.	With respect to the transfer of personal data to third parties it needs to be differentiated between a transfer within the European Economic Area ("EEA") and a transfer to any other country outside the EEA: > - Due to the harmonisation of data protection law by European law, a transfer of personal data to third parties within the EEA is treated as if it took place within the territory of Germany, ie it is admissible if explicitly permitted by the BDSG or any other legal provision or if the data subject has explicitly consented in advance. > - The transfer of personal data to a country outside the EEA ("cross border") is admissible provided the following conditions are fulfilled: >> - regardless of the fact that the personal data is transferred cross border, a legal basis for the transfer as such is required, ie in the absence of consent, it needs to be explicitly permitted by the BDSG or any other legal provision, and >> -the data recipient needs to ensure an adequate level of data protection. The European Commission considers data recipients in Andorra, Switzerland, Canada, Argentina, Guernsey, the Isle of Man, Faeroe Islands, Israel, New Zealand, Jersey and Uruguay as providing such an adequate level (as of 19 January 2016). In case the data recipient is seated in the US, it should comply with the US Department of Commerce's Safe Harbour Privacy Principles. In addition, adequate safeguards with respect to the protection of personal data can be achieved by entering into binding corporate rules (only applicable if the data recipient is a group company) or by entering into a data processing agreement based on the EU model clauses of the European Commission. Please note that a data transfer agreement based on the EU model clauses must be strictly in compliance with the wording of the model clauses provided by the EU Commission. Please note that in the case of transfers of personal data to the US, until 6 October 2015 the adequate level of data protection was acknowledged as ensured at the recipient if the recipient complied with the US Department of Commerce's Safe Harbour Privacy Principles. Following the Judgment of the Court of Justice of the European Union on 6 October 2015 in the case of Schrems (C-362/14) the US-EU Safe Harbour regime is no longer regarded as a valid basis for transferring personal data to the US.Therefore, currently only binding corporate rules and EU model	Under the Guideline, Data Controller may transfer personal data to third parties if the following conditions are met: > - the Data Controller does not transfer in contravention of the transfer purpose notified or outside the scope of transfer notified > - the Data Controller ensures, in contract, the receiver has the capability and is responsible to properly process the personal data in accordance with the Guideline > - personal data will be kept confidential from any individual, organization or facility during the transfer > - Data Controller ensures that the personal information is kept in whole, usable and updated, before and after transfer, and > - unless explicit consent from data subject, express authorization from laws or regulations or authorization from relevant authorities is acquired, personal information must not be transferred to a receiver outside the territory of the People's Republic of China. With respect to transfers, there are no specified requirements in the Decision or the Consumer Rights Law. The Draft Law includes requirements for personal data of Chinese citizens and "important business data" collected by KIIOs to be kept within the borders of the PRC. If there is business needs for the KIIOs to transfer these data outside of China, security assessments must be conducted. This reflects a growing trend towards data localisation in China. The definition of KIIOs remains to be finalised.

7. Security	Most US businesses are required to take reasonable technical, physical and organizational measures to protect the security of sensitive personal information (eg health or financial information, telecommunications usage information, or information that would require security breach notification). A few states have enacted laws imposing more specific security requirements for data elements that trigger security breach notice requirements. For example, Massachusetts has enacted regulations which apply to any company that collects or maintains sensitive personal information (eg name in combination with Social Security number, driver's license, passport number, or credit card or financial account number) on Massachusetts residents. Among other things, the Massachusetts regulations require regulated entities to have a comprehensive, written information security program; the regulations also set forth the minimum components of such program, including binding all service providers who touch this sensitive personal information data to protect it in accordance with the regulations. Both Nevada and Massachusetts laws impose encryption requirements on the transmission of sensitive personal information across wireless networks or beyond the logical or physical controls of an organization, as well as on sensitive personal data stored on laptops and portable storage devices. HIPAA regulated entities are subject to much more extensive data security requirements, and some states impose further security requirements (eg for payment card data, for social security numbers, or to employ secure data destruction methods). HIPAA security regulations apply to so-called 'covered entities' such as doctors, hospitals, insurers, pharmacies and other health-care providers, as well as their 'business associates' which include service providers who have access to, process, store or maintain any protected health information on behalf of a covered entity. 'Protected health information' under HIPAA generally includes any personally identifiable information collected by or on behalf of the covered entity during the course of providing its services to individuals. Federal financial regulators impose extensive security requirements on the financial services sector, including requirements for security audits of all service providers who receive data from financial institutions.	Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as mentioned above, and appropriate to the nature of the data. The Act does not specify specific security measures to adopt and implement. However, the ICO recommends that organisations should adopt best practice methodologies such as ISO 27001.	Data controllers must take appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the harm which might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as mentioned above, and appropriate to the nature of the data. In the frame of the new IT Security Act, which came into force on 25 July 2015, new provisions have been added to the German Telemedia Act (TMG). According to the TMG service providers, e.g. website operators, have to ensure, as far as technically and economically reasonable, by technical and organizational arrangements, that there is no unauthorized access to their technical facilities and that these are secured against violations of the security of personal data as well as against disorders caused by external attacks. Such arrangements have to be of state of the art technology.	Under the Guideline, a Data Controller must take appropriate technical and organizational measures against unauthorized or unlawful processing and against accidental loss, destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the harm that may result from such unauthorized or unlawful processing, accidental loss, destruction or damage, and appropriate to the nature of the data. Furthermore, the Data Controller should: > - plan, design and implement a systemic personal information management process > - design standard personal information management and implement the responsibility of managing personal information > - designate expert institution or personnel to be responsible for the internal management of personal information protection work, available to process data subject complaints or inquiries > - design and implement educational training on personal information protection > - set up an internal management control system for personal information protection, and > - periodically conduct assessment on the status of personal information safety, protection standard and measures implementation either on its own or through an independent evaluation agency. Article 4 of the Decision requires internet service providers and other enterprises to take technical measures and other necessary measures to ensure information safety and prevent the leakage, damage, or loss of citizen electronic information collected in business activities. Where there is a risk or occurrence of information leakage, damaging or loss, remedial measures shall be taken. Article 29 of the Consumer Rights Law requires the same, though as mentioned above, the relevant provision is only applicable to business operators collecting customer personal information. Under the Draft Law, network operators are required to establish information protection systems. In particular, network operators should take technical measures and other necessary measures to ensure the safety of the citizens' personal information and to prevent the collected data from being accidentally disclosed, tampered or destroyed. Remedial measures shall be taken immediately if personal data are being or are likely to be

8. Breach Notification	Security breach notification requirements are a US invention. 47 US states, Washington, D. C. and most US territories (including, Puerto Rico, Guam and the Virgin Islands) require notifying state residents of a security breach involving residents" name plus a sensitive data element typically, social security number, other government ID number, or credit card or financial account number. In a growing minority of states, sensitive data elements also include medical information, health insurance numbers, biometric data, and login credentials (ie username and password). Also, date of birth, tax ID, shared security "secrets", and birth and marriage certificates are each considered sensitive data under the breach notice laws of at least one state. Notice of larger breaches is typically required to be provided to credit bureaus, and in minority of states, to State Attorneys Generals and/or other state officials. Federal laws require notification in the case of breaches of health care information, breaches of information from financial institutions, breaches of telecomm usage information held by telecomm services, and breaches of government agency information.	There is no mandatory requirement in the Act to report data security breaches or losses to the ICO or to data subjects. However, ICO guidance indicates that if a large number of people are affected or the consequences of the breach are particularly serious, the ICO should be informed. Sector specific regulations/guidance do impose obligations to notify the relevant regulator and data subjects in the event of a security breach (eg the Financial Conduct Authority). Mandatory breach notification None contained in the Act. However, the Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PEC Regulations'), as amended, require providers of a public electronic communications service to notify the ICO (and in some cases subscribers) in the event of a personal data breach. Failure to notify can result in a fine of GBP 1,000 and negative publicity.	A breach notification duty has recently been implemented into the BDSG. According to Sec. 42a BDSG the notification duty applies if: > - sensitive personal data, personal data subject to professional secrecy, personal data related to criminal and/or administrative offences, personal data concerning bank or credit card accounts, certain telecommunications and online data is abused or lost and an authorised third party acquires knowledge, and > - in case of telecommunications and online data, there is a serious threat of interference with interests of concerned individuals. Data controllers are obliged to inform supervisory authorities and the concerned individuals.	There is currently no mandatory requirement in PRC law that applies to the public sector to report data security breaches or losses to any authority. The Guideline however recommend that the Data Controller should promptly notify a data breach to affected data subjects and in case of major breach, promptly report to the personal information protection management department. Under the Draft Law, network operators must inform the data subject in the circumstances that the collected personal data are being disclosed and report must be made to the relevant authorities.

9. Enforcement	Violations are generally enforced by the FTC, State Attorneys General, or the regulator for the industry sector in question. Civil penalties are generally significant. In addition, some privacy laws (for example, credit reporting privacy laws, electronic communications privacy laws, video privacy laws, call recording laws, cable communications privacy laws) are enforced through class action lawsuits for significant statutory damages and attorney's fees. Defendants can also be sued for actual damages for negligence in securing personal information such as payment card data, and for surprising and inadequately disclosed tracking of consumers.	In the UK the ICO is responsible for the enforcement of the Act. If the ICO becomes aware that a data controller is in breach of the Act, he can serve an enforcement notice requiring the data controller to rectify the position. Failure to comply with an enforcement notice is a criminal offence and can be punished with fines of up to GBP 5,000 in the Magistrates' Court or with unlimited fines in the Crown Court. The ICO can impose fines of up to GBP 500,000 for serious breaches of the Act. This penalty, introduced in April 2010, can be imposed in respect of breaches of the data protection principles which are: > - serious, and > - likely to cause substantial damage or distress and either >> - the contravention was deliberate, or >> - the data controller knew or ought to have known that there was a risk that the breach would occur and would be likely to cause substantial damage or distress, but failed to take reasonable steps to prevent the breach. Financial services firms regulated by the Financial Conduct Authority (FCA) may find that a breach of the Act may also give rise to enforcement action by the FCA in respect of a breach of the FCA Principles for Business. The FCA enforcement powers are extensive and can include unlimited fines.	Violation of German data protection laws are subject to pecuniary fines up to EUR 300,000 per violation (administrative offence). In the case of wilful behaviour or if conducted in exchange for a financial benefit (criminal offence), by imprisonment of up to 2 years or a fine depending on how severe the violation is. Authorities may also skim profits generated by data protection breaches. In the past, German data protection authorities were rather reluctant concerning the enforcement of data protection law, ie very few official prosecution procedures were opened and imposed fines were rather low. However, this has recently changed and we note a tendency to a stricter enforcement. This particularly relates to several data protection scandals involving loss and disclosure or misuse of personal data in the recent years. Further, reputation damages are usually quite severe if data protection breaches become public. Civil liabilities as well as injunctive reliefs and skimming of profits are likely under the Unfair Competition Act.	Sanctions in relation to data privacy breaches are scattered in different laws and regulations. Typically, it would be graded approach - warning and requirement to comply, then possibly fines up to approximately 500,000 RMB. The affected individuals may also claim for indemnification under the Tort Liability Law. In severe cases, it may lead to higher fines being imposed or the revocation of license. Responsible personnel could be prohibited from engaging in relevant business and their conduct could be recorded into their social credit files. Depending on the severity of the illegal conduct, the responsible person could be subject to detention or up to seven years of imprisonment, plus a concurrent fine to the organization if applicable. China currently lacks an efficient and centralised enforcement mechanism for data protection and there is no data protection authority or any other state agency established to monitor the protection of personal data. The data protection provisions provided by the Criminal Law have become the most widely used provisions to enforce privacy protection in China. Essentially, only to the illegal sale or purchase of personal data are subject to enforcement under the Criminal Law. The Draft Law also suggest possibility of ordering corrections or issuing warnings upon discovery of violation in handling personal data. If serious or poses threat to network security, varying levels of fines between $10,000 and $500,000 may be charged, and possible suspension of permits or licenses depending on the level of non-compliance. Please note again that the possible enforcements in light of a data privacy breach discussed here are not comprehensive in all situations, as additional laws or regulations may be applicable depending on the industry or type of information at hand.

10. Electronic Marketing	The US regulates marketing communications extensively, including email and text message marketing, as well as telemarketing and fax marketing. E-mail The CAN-SPAM Act is a federal law that applies labelling and opt-out requirements to all commercial email messages. CAN-SPAM generally allows a company to send commercial emails to any recipient, provided the recipient has not opted out of receiving such emails from the sender, the email identifies the sender and the sender's contact information, and the email contains instructions on how the recipient can easily and without cost opt out of future commercial emails from the sender. Not only the FTC and State Attorneys General, but also ISPs and corporate email systems can sue violators. Furthermore, knowingly falsifying the origin or routing of a commercial email message is a federal crime. Text Messages Federal and state regulations apply to the sending of marketing text messages to individuals. Express consent is required to send text messages to individuals, and, for marketing text messages, express written consent is required (electronic written consent is sufficient, but verbal consent is not). The applicable regulations also specify the form of consent. This is a significant class action risk area, and any text messaging (marketing or informational) needs to be carefully reviewed for strict compliance with legal requirements. Telemarketing In general, federal law applies to most telemarketing calls and programs, and a state's telemarketing law will apply to telemarketing calls placed to or from within that particular state. As a result, most telemarketing calls are governed by federal law, as well as the law of one or more states. Telemarketing rules vary by state, and address many different aspects of telemarketing. For example, national ('federal') and state rules address calling time restrictions, honouring do-not-call registries and opt-out requests, mandatory disclosures to be made during the call, requirements for completing a sale, executing a contract or collecting payment during the call, restrictions on the use of auto-dialers and pre-recorded messages, and record keeping requirements. Many states also require telemarketers to register or obtain a license to place telemarketing calls. Callers generally must scrub their calling lists	The Act will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (eg an email address is likely to be 'personal data' for the purposes of the Act). The Act does not prohibit the use of personal data for the purposes of electronic marketing but provides individuals with the right to prevent the processing of their personal data (eg a right to 'opt-out') for direct marketing purposes. There are a number of different opt-out schemes/preference registers for different media types. Individuals (and, in some cases, corporate subscribers) can contact these schemes and ask to be registered as not wishing to receive direct marketing material. If advertising materials are sent to a person on the list, sanctions can be levied by the ICO using his powers under the Act. The PEC Regulations prohibit the use of automated calling systems without the consent of the recipient. The PEC Regulations also prohibit unsolicited electronic communications (ie by email or SMS text) for direct marketing purposes without prior consent from the consumer unless: > - the consumer has provided their relevant contact details in the course of purchasing a product or service from the person proposing to undertake the marketing > - the marketing relates to offering a similar product or service, and > - the consumer was given a means to readily 'opt out' of use for direct marketing purposes both at the original point where their details were collected and in each subsequent marketing communication. Each direct marketing communication must not disguise or conceal the identity of the sender and include the 'unsubscribe' feature referred to above. The restrictions on marketing by email / SMS only applies in relation to individuals and not where marketing to corporate subscribers.	In general, unsolicited electronic marketing requires prior opt-in consent. The opt-in requirement is waived under the 'same service/product' exemption. The exemption concerns marketing emails related to the same products/services as previously purchased from the sender by the user provided: > - the user has been informed of the right to opt-out prior to the first marketing email > - the user did not opt-out, and > - the user is informed of the right to opt-out of any marketing email received. The exemption applies to electronic communication such as electronic text messages and email but does not apply with respect to communication sent by fax. Direct marketing emails must not disguise or conceal the identity of the sender.	Under the Decision, any organizations and individuals are forbidden from acquiring personal electronic information by theft or other illegal methods. Also, they are proscribed from selling or unlawfully providing personal electronic information to anyone else. Network service providers will require users to provide genuine identification information when signing agreements to grant them access to the Internet, fixed-line telephone or mobile phone services or to permit users to make information public. The Decision prohibits any organizations and personnel from sending commercial electronic information to a personal fixed-line telephone, mobile phone or email address without the consent or request of the electronic information recipient, or where the recipient has explicitly declined to receive such information. The Consumer Rights Law prohibits sending of commercial information where the customer has not consented, made any request to receive the information, or where the customer has explicitly stated refusal to receive the information. The Cyberspace Administration of China ("CAC") has recently released the "Provisions on Administration of Internet Information Search Services". The stricter internet advertising regulation comes into force on August 1, 2016 and requires Internet search providers to ensure objective, fair and authoritative search results and remove any illegal content. Service providers are obliged to establish an information security management system to protect personal information and regularly examine the qualifications of public information. All pay-for-performance searches need to be clearly labeled on an item by item basis. Additionally, proposals for accompanying draft rules to a draft Civil Code suggest the possibility of treating data as intellectual property. This indicates, once the law is passed, that data may be traded by organizations for marketing purposes. The draft rules may not be approved until early 2017, and the forthcoming Civil Code is expected to be approved in 2020. Further developments are awaited on these.

11. Online Privacy	Online Privacy Policy Requirement The States of California and Delaware require commercial online websites and mobile applications to post a relatively general online privacy policy. Liability for failing to post the privacy policy may only be imposed if the website or mobile app is notified of its non-compliance and fails to post the policy with 30 days of receiving notice of non-compliance. Cookies There is no specific federal law that regulates the use of cookies, web beacons, Flash LSOs and other similar tracking mechanisms. However, the Children's Online Privacy Protection Act (COPPA) applies to information collected automatically (eg via cookies) from child-directed websites and other websites and third party ad networks or plug-ins that knowingly collect personal information online from children under 13, COPPA also regulates behavioural advertising to children under 13. In addition, undisclosed online tracking of customer activities poses class action risk. The use of cookies and similar tracking mechanisms should be carefully and fully disclosed in a website privacy policy. Furthermore, it is a best practice for websites that allow behavioural advertising on their websites to participate in the Digital Advertising Alliance code of conduct, which includes displaying an icon from which users can opt out of being tracked for behavioural advertising purposes. Under California law, any company that tracks any personally identifiable information about consumers over time and across multiple websites must disclose in its privacy policy whether the company honours any 'Do-Not-Track' method or provides users a way to opt out of such tracking; however, the law does not mandate that companies provide consumers a 'Do-Not-Track' option. The same law also requires website operators to disclose in their privacy policy whether any third parties may collect any personally identifiable information about consumers on their website and across other third party websites, and prohibits the advertsing of certain products, services and materials (including alcohol, tobacco, firearms, certain dietarty supplements, ultraviolet tanning, tattoos, obscene matters, etc). Minors California law requires that operators of websites or online services that are directed to minors or that knowingly collect personally identifiable information from minors permit	The PEC Regulations (as amended) deal with the collection of location and traffic data by public electronic communications services providers ('CSPs') and use of cookies (and similar technologies). Traffic Data Traffic Data held by a CSP must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication. However, Traffic Data can be retained if: > - it is being used to provide a value added service, and > - consent has been given for the retention of the Traffic Data. Traffic Data can also be processed by a CSP to the extent necessary for: > - the management of billing or traffic > - dealing with customer enquiries > - the prevention of fraud, or > - the provision of a value added service. Cookie Compliance The use and storage of cookies and similar technologies requires: > - clear and comprehensive information, and > - consent of the website user. The ICO has confirmed that consent can be implied where a user proceeds to use a site after being provided with clear notice (eg by way of a pop-up or banner) that use of site will involve installation of a cookie. Consent is not required for cookies that are: > - used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or > - strictly necessary for the provision of a service requested by the user. Enforcement of a breach of the PEC Regulations is dealt with by the ICO and sanctions for breach are the same as set out in the enforcement section above.	Traffic data Traffic data qualifies as personal data. Providers of telecommunication services may collect and use the following traffic data to the following extent: > - the number or other identification of the lines in question or of the terminal > - authorisation codes, additionally the card number when customer cards are used > - location data when mobile handsets are used > - the beginning and end of the connection, indicated by date and time and, where relevant to the charges, the volume of data transmitted > - the telecommunications service used by the user > - the termination points of fixed connections, the beginning and end of their use, indicated by date and time and, where relevant to the charges, the volume of data transmitted. Any other traffic data required for setup and maintenance of the telecommunications connection and for billing purposes. Stored traffic data may be used after the termination of a connection only where required to set up a further connection, for billing purposes or in case the user has requested a connection overview. The service provider may collect and use the customer data and traffic data of subscribers and users in order to detect, locate and eliminate faults and malfunctions in telecommunications systems. This applies also for faults, which can lead to a limitation of availability of information and communications systems or which can lead to an unauthorized access of telecommunications and data processing systems of the users. Otherwise, traffic data must be erased by the service provider without undue delay following termination of the connection. Service providers have to inform the users immediately, if any faults of data procession systems of the users become known. Furthermore the service provider has to inform the users about measures for detecting and rectifying faults. Location Data Location Data qualifies as personal data. This data may only be processed as required for the provision of requested	Article 3 of the Decision indicates that network service providers and other companies should ensure the privacy of personal electronic information. They are not allowed to disclose, falsify, damage, as well as sell or unlawfully provide personal electronic information to anyone else. Article 29 of the Consumer Rights Law offers similar protection to consumer personal information as well. Article 5 of the Decision indicates that network service providers should strengthen management of information issued by users. Also, network service providers should stop the transmission of unlawful information and take necessary measures to remove them and save relevant records, then report to supervisory authorities. Once citizens find network information that discloses their identity or breaches their legal rights, or are harassed by commercial electronic information, they have the right to require that the network service provider delete related information or take measures to prevent such behaviors. In relation to online privacy on mobile apps, it is, however, required by the "Provisions on Administration of Information Services of Mobile Internet Application Programs" that app providers adopt real-name registrations and verity users' identities based on mobile phone numbers or other information. Providers are prohibited from collecting users' location data, reading their contacts, starting the recording function or camera or any other irrelevant functions without clear notification and users' consent. Furthermore, App publishers are required to undertake information content review and management mechanism including to punish anyone releasing illicit information through warnings, limitation of functions, cease updates, or shutting down accounts. There are currently no specific requirements regarding cookies within existing laws or regulations in the PRC.

	Source : https://www.dlapiperdataprotection.com