Quality online panels. Proven results.®

2011

Laws & Regulations

Laws and regulations can be categorized into the following areas.

Information Protection	Laws governing the use, storage, and transmission of individual identifiable information. The laws concentrate the protection of individual information by establishing responsibility of the data guardian to: • Have a clear intent and use of the information. The organization is expected to use the information for the intended purpose for fair and lawful means. • Establish responsibility within the organization for information security and protection • Implement appropriate security measures and restrict access to limit exposure and safeguard the information • Ensure the information is accurate, complete, and current based on the need and usage of the information • Obtain consent when collecting, disclosing, and using the information • Provide a means to restrict the usage or withdraw the information
Financial Reporting	Financial reporting laws focus on the financial significant systems and general Information technology controls to minimize the risk of events that could lead to a material misstatement of the company's financials. Information technology controls provide a layer of assurance of the reliance for the financial statements. The IT controls safeguards the likelihood of an error that would be material to the financial transactions and reporting. A majority of country financial reporting laws are based on the US Sarbanes-Oxley law. Guidelines for these laws require: • A yearly risk assessment to establish the priorities for business controls. The business should establish a limited number of key controls that will prevent and detect material errors. • Definition of business processes with adequate controls • Maintain operational records as evidence to the effectiveness of the business controls • A constant management oversight and review of the business controls • Execute controls flawlessly. Controls established by management are considered essential in establishing reliability of the financial statements. Therefore, the tolerance level of not executing the controls is low.
Safe Harbor	under which participating US companies can receive data if they promise to abide by rules over and above US law Where an organization is subject to US statutory, regulatory, administrative or other body of law (or body of rules issued by national securities exchanges, registered securities associations, registered clearing agencies, or a Municipal Securities Rule-making Board) that also effectively protects personal data

	privacy, it qualifies for the safe harbor to the extent that its activities are governed by such laws or rules. Organizations may also put in place the safeguards deemed necessary by the EU for transfers of personal data from the EU to the US by incorporating the relevant safe harbor principles into agreements entered into with parties transferring personal data from the EU.(1)* **Safe Harbor Principles** **1. NOTICE:** An organization must inform individuals about the purposes for which it collects information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or discloses it to a third party. **2. CHOICE:** An organization must offer individuals the opportunity to choose (opt out) whether and how personal information they provide is used or disclosed to third parties (where such use is incompatible with the purpose for which it was originally collected or with any other purpose disclosed to the individual in a notice). They must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise this option. For sensitive information, such as medical and health information, information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information concerning the sex life of the individual they must be given affirmative or explicit (opt in) choice.(4) **3. ONWARD TRANSFER:** An organization may only disclose personal information to third parties consistent with the principles of notice and choice. Where an organization has not provided choice because a use is compatible with the purpose for which the data was originally collected or which was disclosed in a notice and the organization wishes to transfer the data to a third party, it may do so if it first either ascertains that the third party subscribes to the safe harbor principles or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant safe harbor principles.(5) **4. SECURITY:** Organizations creating, maintaining, using or disseminating personal information must take reasonable measures to assure its reliability for its intended use and reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction. **5. DATA INTEGRITY:** Consistent with these principles, an organization may only process personal information relevant to the purposes for which it has been gathered. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is accurate, complete, and current. **6. ACCESS:** Individuals must have [reasonable] access to personal information about them that an organization holds and be able to correct or amend that information where it is inaccurate. [Reasonableness of access depends on the nature and sensitivity of the information collected, its intended uses, and the expense and difficulty of providing the individual with access to the

	information.](6) **7. ENFORCEMENT:** Effective privacy protection must include mechanisms for assuring compliance with the safe harbor principles, recourse for individuals to whom the data relate affected by non-compliance with the principles, and consequences for the organization when the principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which an individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with these principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.
Children online Privacy	Unlawful for any operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from… • Obtain verifiable parental consent prior to the collection, use, and disclosure of information about a minor. • Provide notice on the website of what information is collected from the minor, how the information is used, and disclosure practices. • Provide, upon requested of a parent, a description of the types of information collected, use and disclosure practices • Provide a parent the opportunity to refuse and remove a child's information and participation in the collection of information.
Spam Laws	Commercial messages sent via electronic mail messages for advertisement, promotion, product or service information and messages that promote websites fall under country spam laws. Guidelines for commercial messages include: 1. **Don't use false or misleading header information.** Your "From," "To," "Reply-To," and routing information – including the originating domain name and email address – must be accurate and identify the person or business who initiated the message. 2. **Don't use deceptive subject lines.** The subject line must accurately reflect the content of the message. 3. **Identify the message's purpose.** Spam laws give leeway in how the purpose is defined, but you must disclose clearly and conspicuously especially if your message is an advertisement. 4. **Tell recipients where you're located.** The message must include the organization's valid physical postal address. This can be your current street address, a post office box you've registered with the U.S. Postal Service, or a private mailbox you've registered with a commercial mail receiving agency established under Postal Service regulations.

	5. **Tell recipients how to opt out of receiving future email from you.** Your message must include a clear and conspicuous explanation of how the recipient can opt out of getting email from you in the future. Craft the notice in a way that's easy for an ordinary person to recognize, read, and understand. Creative use of type size, color, and location can improve clarity. Give a return email address or another easy Internet-based way to allow people to communicate their choice to you. You may create a menu to allow a recipient to opt out of certain types of messages, but you must include the option to stop all commercial messages from you. Make sure your spam filter doesn't block these opt-out requests. 6. **Honor opt-out requests promptly.** Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your message. You must honor a recipient's opt-out request within 10 business days. You can't charge a fee, require the recipient to give you any personally identifying information beyond an email address, or make the recipient take any step other than sending a reply email or visiting a single page on an Internet website as a condition for honoring an opt-out request. Once people have told you they don't want to receive more messages from you, you can't sell or transfer their email addresses, even in the form of a mailing list. The only exception is that you may transfer the addresses to a company you've hired to help you comply with the spam law. 7. **Monitor what others are doing on your behalf.** Spam laws make it clear that even if you hire another company to handle your email marketing, you can't contract away your legal responsibility to comply with the law. Both the company whose product is promoted in the message and the company that actually sends the message may be held legally responsible.
Privacy Rights	Businesses are required to provide to their customers their privacy policy Required to notify individuals of security breach involving personal private information (PPI) or Personal Identifiable Information (PII) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or edacted: 1) Social Security number 2) Driver's license number or State identification card number. 3) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. Personally identifiable information is defined as any information relating to an

	identified or identifiable individual. Such information includes, but is not limited to, the customer's name, address, telephone number, social security/insurance or other government identification numbers, employer, credit card numbers, personal or family financial information, personal or family medical information, employment history, history of purchases or other transactions, credit records and similar information. Sensitive information is defined as personally identifiable information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or sexual preferences.
Notification	Required to notify customers (at customer's request) the names of third parties that have received personal information including information relating to income or purchases for direct marketing purposes Individuals have the right to know whether information concerning them is being processed and to obtain a copy of the information in an intelligible form.
Spyware	These laws make it illegal for anyone other than the owner or operator of a computer to install software that monitors web browser settings, monitors keystrokes, or disables security settings. To be compliant a user must explicitly consent to an end user license agreement during installation or terms of use that include the use of tracking software.
Data transmission	Confidentiality of communication s is guaranteed in accordance with the i Comparable safeguards for protection of privacy must be taken and ensured when transmitting data across borders. If safeguards are not reciprocal then limitations on content should be administered.
Search and Seizure	Many countries restrict search and seizure regulations that limit a government to obtain information. 1. Where it is feasible, a search must be approved by prior authorization. Although it may not always be reasonable to insist on prior authorization, there will be a presumption that a warrantless search is unreasonable. 2. The person authorizing the search must act in a judicial manner. Although the person need not be a judge, he or she must be in a position to assess in a neutral and impartial fashion whether a search is appropriate on the evidence available. 3. The standard for issuance of the warrant is similar to American "probable cause": There must be reasonable and probable grounds established upon oath to believe that an offence has been committed, and that evidence of that offense is to be found at the place to be searched.
Technology Import / Export	A small percentage of items requires export and import license. Items for reasons of national security, nonproliferation, foreign policy, and short supply may require a license. Licenses are dependent upon the technical characteristics, destination, use, and recipient of the item.

	Electronic items, including hardware and software, fall under export rules when: • Taken electronic equipment and software abroad • Allow a person in a foreign country to use their electronic equipment • Allow a foreign national access to their electronic equipment even while the equipment remains in the origin country ("Deemed Export") Electronic items should be classified under the origination and destination country's export classification scheme to determine export constraints. Most of e-Rewards electronic hardware, software and information are not restricted or require export or import licenses.
Information Retention and Destruction	Information retention laws vary from country to country and based on the type of information. For example employment, financial, and legal records have defined laws requiring their retention. An important aspect of these laws is information classification and retention. Sensitive information must be identified and protected. Records are business information that must be kept for regulatory, legal, or operational reasons. Electronic records should be managed, classified, and have a defined retention period. Electronic media used to store information follow a lifecycle of purchased, in use, obsolete and destroyed or surplus. Electronic media that is identified as obsolete should be completely erased so that no information is accessible prior to redeployed or disposed.
Outsourcing	The European Commission has updated the Data Protection Directive standard contractual clauses for the transfer of personal data outside the European Union in response to changes in the way that businesses manage data. The new contractual clauses demand greater transparency from overseas companies providing data processing operations to clients in the EU, requiring them to obtain written consent before subcontracting any processing of personal data to another firm. **For transfers to all other countries (exclude: Switzerland, Canada, Argentina, Guernsey, the Isle of Man and Jersey), there must be specific data protection contractual arrangements in place before the personal data of EU residents can be sent to companies based there for processing. The European Commission produces standard clauses that are used in such contracts.**

Multiple Country Support

Individual countries may have regulations and statutes that conflict, limit or prohibit the transfer of information and technology between countries. The following table identifies country regulations that may restrict inter-country business.

Country	Regulation	Impact

US	NAFTA Export Reg: Patriot Act Foreign Corrupt Practices Act	Movement of assets Transfer of technology Licensing Information protection US has Safe Harbor laws that allow information to be transmission with EU and other countries
Argentina		
Australia		
Austria		
Barbados		
Belgium		
Brazil		
Bulgaria		
Canada	Bill 161 – An Act to establish a legal framework for information technology	Canada has restrictions of what type of information may be accessable from US networks to ensure that the US Patriot Act does not violate Canada Search and Seizure laws
Central African Republic		
Chile		
China		
Colombia		
Croatia		
Cyprus		
Czech Republic		
Denmark		
Egypt		
Estonia		
European Union		Countries are implementing laws requiring certification of information protection measures at an organization and country infrastructure level. The EU has placed restrictions from outsourcing information services that have third world countries from receiving and storing PII data. EU has Safe Harbor laws that allow information to be transmission with US

Finland		
France		
Germany		
Greece		Information is restricted for being transmitted (exported) across country borders
Hong Kong		
Hungary		
Iceland		
India		
Indonesia		
Ireland		
Israel		
Italy		
Jamaica		
Japan		
Kenya		
Kuwait		
Latvia		
Malaysia		
Mexico		
Netherlands		
New Zealand		
North Korea		
Norway		
Peru		
Philippines		
Poland		
Portugal		
Puerto Rico		
Romania		
Russia		
Saudi Arabia		
Singapore		

Slovakia		
South Africa		
South Korea		
Spain		
Swaziland		
Sweden		
Switzerland		
Taiwan		
Thailand		
Turkey		
Ukraine		
United Arab Emirates		
United Kingdom		
United Nations		
Venezuela		
Vietnam		

International Directives

Regulation	Impact	Countries
OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data	The development of automatic data processing, which enables vast quantities of data to be transmitted across national borders has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD Member countries to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data,	Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain and Switzerland have prepared draft bills

	or the abuse or unauthorized disclosure of such data.	
Wassenaar Arrangement	International, multilateral arrangement that outlines the export controls, exchange of views and information, and technology transfer throughout the world	Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, United States

Outsourcing Services

The business has established an outsourcing strategy for survey job development and operations being executed in India. The following steps need to be included in the outsourcing project:

- Contractual language for customer, partner, and outsourcing company needs to be included in new agreements. An evaluation of existing contracts should be conducted to determine whether updates to the agreements are required
- Security assessment of the outsourcing company's facilities and operations should be conducted
- Outsourcing certifications such as SAS 70 should be obtained and updated on a regular basis
- An analysis of country restrictions of using an outsourcing service should be conducted and guidelines established for business operations