

ANNUAL LEGAL UPDATE

Recent and Upcoming Legislative Changes – United States

Country / Jurisdiction	Bill / Statute Reference	Effective / Enacted Date	Impact	Description
United States	Alabama HB 56	Effective April 1, 2012	E-Verify	<p>This law requires all Alabama employers, private and public, to enroll in E-Verify by January 1, 2012 and begin using it no later than April 1, 2012. This law also prohibits employers from hiring illegal immigrants, which is similar to the Arizona’s controversial immigration law SB 1070.</p> <p>Please refer to the text on Alabama HB 56 for more details.</p>
United States	California AB 22	Effective January 1, 2012	Credit Check	<p>This law was passed in October 2011 but went into effect January 1, 2012, restricting an employer’s use of credit reports in making hiring decisions. This law prohibits California employers from utilizing a credit report in making a hiring decision unless the position is included as one of the acceptable positions outlined in the statute, the candidate is provided written notification that such a report may be obtained, and the candidate provides their consent. In addition, if the employer obtains the credit report for one of the permitted positions, it must also provide the consumer with the specific reasons why such a report will be collected and have a checkbox allowing the candidate to request a copy of the credit check free of charge. Accurate Background is providing a sample Disclosure and Authorization form which is compliant with this new statute for your reference. For more information regarding this legislative change, please view the original Legislative Update we sent out in October 2011.</p>
United States	California SB 909	Effective January 1, 2012	Disclosure	<p>California Senate Bill 909 requires California employers to provide additional disclosures to job applicants if the background screening provider is sending personal data outside of the United States for domestic searches. For example, this regulation is imposed if the background screening provider outsources customer service to a call center in another country and that call center is given access to the applicant's personally identifiable information (PII) such as SSN or date of birth. Accurate Background never off-shores an applicant's personal information if their address history and experience (i.e. education / employment) is solely domestic. In addition, our standard Disclosure and Authorization forms include full contact information for Accurate Background as required by CA SB 909.</p>

Please note: The information provided above is strictly for educational purposes. It is not intended to be legal advice, either expressed or implied. Accurate Background recommends that you consult with your legal counsel regarding all employment regulations.

ANNUAL LEGAL UPDATE



Country / Jurisdiction	Bill / Statute Reference	Effective / Enacted Date	Impact	Description
United States	DE Executive Order 2012-3	Passed December 6, 2012	Ban the Box	<p>The executive order requires removal of the criminal conviction history question from the City's non-uniformed employment applications. Criminal background checks will only be conducted on applicants who have received a conditional offer of employment. There are exclusions as it relates to safety positions such as police and fire.</p> <p>Additional information may be found at: http://www.ci.wilmington.de.us/news/news.php?newsID=640</p>
United States	EEOC Guidance	Effective April 25, 2012	EEOC	<p>The EEOC released additional guidance on an employer's use of a candidate / employee's criminal history in a hiring decision. Although this guidance is not law, it is designed to provide the standards and criteria that will be followed in EEOC enforcement actions, including in U.S. Courts.</p> <p>The EEOC has previously indicated that employers should take into consideration the "green factors:"</p> <ul style="list-style-type: none"> ▪ The nature and gravity of the offense ▪ The time that has passed since the conviction and/or completion of sentence ▪ The nature of the job sought or held <p>Additionally, the EEOC encouraged all employers to use either a validation study or a targeted screen, including a personal assessment, regarding criminal offenses.</p> <p>Some of the best practices discussed in the Guidance include:</p> <ul style="list-style-type: none"> ▪ Eliminate policies or practices that exclude people from employment based on any criminal record; ▪ Train managers, hiring officials, and decision makers about Title VII of the Civil Rights Act and its prohibition on employment discrimination; ▪ Develop a narrowly tailored written policy and procedure for screening applicants and employees for criminal conduct which may include the following: <ul style="list-style-type: none"> ✓ Identify essential job requirements and the actual circumstances under which the jobs are performed. ✓ Determine the specific offenses that may demonstrate unfitness for performing such jobs.

Please note: The information provided above is strictly for educational purposes. It is not intended to be legal advice, either expressed or implied. Accurate Background recommends that you consult with your legal counsel regarding all employment regulations.

ANNUAL LEGAL UPDATE



Country / Jurisdiction	Bill / Statute Reference	Effective / Enacted Date	Impact	Description
				<ul style="list-style-type: none"> <ul style="list-style-type: none"> ▪ Identify the criminal offenses based on all available evidence. ✓ Determine the duration of exclusions for criminal conduct based on all available evidence. <ul style="list-style-type: none"> ▪ Include an individualized assessment. ✓ Record the justification for the policy and procedures. ✓ Note and keep a record of consultations and research considered in crafting the policy and procedures. ▪ Train managers, hiring officials, and decision makers on how to implement the policy and procedures consistent with Title VII; ▪ When asking questions about criminal records, limit inquiries to records for which exclusion would be job related and consistent with business necessity. ▪ Keep information about applicants' and employees' criminal records confidential. Only use it for the purpose for which it was intended. <p>A summary of the requirements may be read at: http://www.accuratebackground.com/images/sections/eeocguidancemay12.pdf</p> <p>The complete Guidance may be accessed at: http://www.eeoc.gov/laws/guidance/arrest_conviction.cfm</p>
United States	Federal	January 1, 2013	FCRA	<p>All FCRA forms (including the Summary of Rights, Notice to Users of Consumer Reports, Identity Theft Rights, and Notice to Furnishers) must be updated accordingly as required by the Consumer Financial Protection Bureau.</p> <p>https://www.accuratebackground.com/images/sections/cfpblegalupdate.pdf</p>

Please note: The information provided above is strictly for educational purposes. It is not intended to be legal advice, either expressed or implied. Accurate Background recommends that you consult with your legal counsel regarding all employment regulations.

ANNUAL LEGAL UPDATE



Country / Jurisdiction	Bill / Statute Reference	Effective / Enacted Date	Impact	Description
United States	Massachusetts Criminal Offender Record Information (CORI)	Effective May 4, 2012	Criminal Records	<p>The final Massachusetts CORI Reform regulations were issued on May 25, 2012 although the legislation went into effect May 4, 2012. The changes include, but are not limited to, the following:</p> <ul style="list-style-type: none"> ▪ Increased access to criminal record information maintained by the Department of Criminal Just Information Services (DCJIS) ▪ New procedures to access an individual’s criminal record through DCJIS which include a new CORI Acknowledgement form and verification of the individual’s identity ▪ Utilizing a consumer reporting agency (CRA) in requesting CORI information is limited ▪ Adverse action procedures are more complex whether or not the information is obtained from DCJIS or another source. In addition to the adverse action requirements under the Fair Credit Reporting Act (FCRA), Massachusetts law requires notification of the potential adverse decision, a copy of the employer’s background check policy and the document, “Information on how to correct a criminal record.” ▪ Employers who conduct 5 or more criminal background checks each year, whether from DCJIS or another source, must maintain a criminal offender record information policy. A sample policy was provided as a reference, but an employer’s policy should reflect their particular procedures. ▪ Employers must register for iCORI access each year and attend annual training. ▪ Additional requirements are established regarding dissemination, storage, and retention of criminal record information. ▪ DCJIS may audit employers with respect to CORI and individuals. <p>The regulations may be read at: http://www.mass.gov/eopss/docs/chsb/803-cmr-2-00-criminal-offender-record-information-cori.pdf</p> <p>A Summary may be found at: http://www.accuratebackground.com/images/sections/1104101.pdf</p>

Please note: The information provided above is strictly for educational purposes. It is not intended to be legal advice, either expressed or implied. Accurate Background recommends that you consult with your legal counsel regarding all employment regulations.

ANNUAL LEGAL UPDATE



Country / Jurisdiction	Bill / Statute Reference	Effective / Enacted Date	Impact	Description
United States	NC HB 36	<ul style="list-style-type: none"> October 1, 2012, for employers with 500 or more employees. 	E-Verify	<p>This bill was passed in 2011, requiring all cities, counties and businesses with 25 or more employees to utilize E-Verify.</p> <p>Effective dates:</p> <ul style="list-style-type: none"> October 1, 2012, for employers that have 500 or more employees. January 1, 2013, for employers that have between 100 and 499 employees. July 1, 2013, for employers that have between 25 and 99 employees. Agricultural companies hiring seasonal workers for 90 days or less during a 12 consecutive month period will be exempt <p>The bill can be read at: http://www.ncga.state.nc.us/Sessions/2011/Bills/House/PDF/H36v7.pdf</p>
United States	Newark Ordinance #12-1630	Effective November 18, 2012	Ban the Box Criminal Records	<p>For employers with five or more employees and do business, employs persons, or takes applications for employment within the City of Newark, certain restrictions and requirements have been implemented stating that employers may not:</p> <ul style="list-style-type: none"> Conduct a background check on any person pre-application or on candidates unless strict procedures are followed Inquire into an individual's criminal history before an offer has been accepted Make employment decisions on: <ul style="list-style-type: none"> ✓ arrest information that is no longer pending and did not result in a conviction ✓ Records that have been erased, expunged, or otherwise nullified ✓ Sealed juvenile records Create or distribute advertisements that indicate any limitation on eligibility for employment based on criminal history Conduct a criminal record check unless they make a good faith determination that the position is of such sensitivity that a check is warranted

Please note: The information provided above is strictly for educational purposes. It is not intended to be legal advice, either expressed or implied. Accurate Background recommends that you consult with your legal counsel regarding all employment regulations.

ANNUAL LEGAL UPDATE



Country / Jurisdiction	Bill / Statute Reference	Effective / Enacted Date	Impact	Description
				<ul style="list-style-type: none"> If an employer considers an individual's criminal history in a hiring decision, they must consider a list of factors listed in the ordinance, which are included as part of the required Applicant Criminal Record Consideration form. An employer must follow strict procedures if they decide to take an adverse action employment decision based on the individual's criminal check. <p>Additional information and details may be found at: https://www.accuratebackground.com/images/sections/newarklegalupdate.pdf</p>
United States	Pittsburgh Ordinance 2012-0013 and Pittsburgh Ordinance 2012-0015	Passed December 17, 2012	Ban the Box	<p>The City of Pittsburgh city government has passed an ordinance to "ban the box." This will prohibit the City from having the check box asking about an individual's criminal history on their employment application for city positions. There are exclusions for this ordinance for safety sensitive positions, such as the police.</p> <p>There is a second ordinance which requires the same requirements for any contractors and/or vendors doing business in the City of Pittsburgh. Similarly, there are exceptions to this Ordinance as well.</p>
United States	SC H 4400	Effective January 1, 2012	E-Verify	<p>The law, which was passed June 27, 2011, states that all employees must go through the new E-Verify system within three days of hire. A business that fails to comply with the new law may have its business license suspended by the state. Previously, public employers only were required to use E-Verify. Also, employers may no longer verify new employees' employment authorizations status by checking the driver's license or state identification card.</p> <p>http://www.ncsl.org/?tabid=13127</p>

Please note: The information provided above is strictly for educational purposes. It is not intended to be legal advice, either expressed or implied. Accurate Background recommends that you consult with your legal counsel regarding all employment regulations.

ANNUAL LEGAL UPDATE



Country / Jurisdiction	Bill / Statute Reference	Effective / Enacted Date	Impact	Description
United States	TN Lawful Employment Act	Effective: January 1, 2012 for all state and local government agencies and all private employers with 500 or more employees July 1, 2012 for all private employers with 200-499 employees July 1, 2013 for all employers with 6 to 199 employees	I-9 / E-Verify	<p>The Tennessee Lawful Employment Act requires verifying the employment eligibility of all newly hired employees through the online E-Verify program (www.uscis.gov/everify), OR requesting all newly hired employees to provide one of the following identity and employment authorization documents as required:</p> <ul style="list-style-type: none"> ▪ A valid Tennessee driver's license or photo identification ▪ A valid driver's license or photo identification from another state where the license requirements are at least as strict as those in Tennessee ▪ A birth certificate issued by a U.S. state, jurisdiction or territory ▪ A U.S. government issued certified birth certificate ▪ A valid, unexpired U.S. passport ▪ A U.S. certificate of birth abroad ▪ A report of birth abroad of a citizen of the U.S. ▪ A certificate of citizenship ▪ A certificate of naturalization ▪ A U.S. citizen identification card ▪ A lawful permanent resident card <p>The law also requires employers to obtain and maintain a copy of one of the above listed identity/employment authorization documents for all non-employees as well. A "non-employee" is defined as any individual, other than an employee, paid directly by the employer in exchange for the individual's labor or services.</p> <p>http://www.tn.gov/labor-wfd/eVerify/</p>
United States	WA Initiative 1163	Effective January 2, 2012	Homecare	<p>Referred to as the Washington Long-term Care law for serving elderly and persons with disabilities, it requires caregivers, including home care workers, to receive 75 hours of training and undergo an FBI check. There is uncertainty how this will be funded.</p> <p>http://www.sos.wa.gov/elections/initiatives/text/i1163.pdf</p> <p>Service Employees International Union (SEIU) supported the bill</p>

Please note: The information provided above is strictly for educational purposes. It is not intended to be legal advice, either expressed or implied. Accurate Background recommends that you consult with your legal counsel regarding all employment regulations.

ANNUAL LEGAL UPDATE



Recent and Upcoming Legislative Changes - International

Country / Jurisdiction	Bill / Statute Reference	Effective / Enacted Date	Impact	Description
Australia	Privacy Amendment (Enhancing Privacy Protection) Bill 2012	Passed November 29, 2012; Effective March 2014	Personal information, public records and verifications	<p>This bill updates the Privacy Act 1988 and is designed to enhance Australia's protection of personal information. The law will give the nation's privacy commissioner new powers, including the ability to pursue civil penalties in serious privacy breach incidents. The commissioner will also be granted the right to conduct privacy assessments for both public and private organizations in Australia. The reforms introduce a single set of privacy principles called the Australian Privacy Principles (APPs) and a number of changes to how personal information is handled, including when it can be sent overseas.</p> <p>More information can be found at: http://www.computerworld.com.au/article/443247/privacy_amendment_bill_passed_gives_commissioner_far-reaching_powers/</p>
Chile	Law 20575 ("Dicom Law")	Passed February 20, 2012	Credit Reports	<p>This reform legislation, known as the "Dicom" law after Chile's Dicom credit reporting agency, prohibits the use of credit reports for such purposes as emergency health care, selection of persons for employment, and school applications. The new law restricts reporting to matters of "commercial/business risk" and applications for credit.</p>
China	Decision to strengthen the protection of online information	Passed December 28, 2012	Personal Information	<p>Chinese lawmakers have approved rules to increase personal data protection online. The 12-article decision on strengthening online information protection, which has the same legal effect as a law, was adopted at the closing meeting of a five-day session of the Standing Committee of the National People's Congress. The rules are designed to protect personal information security, establish a network identity management policy, clarify the duties of service providers, and endow government watchdogs with necessary supervisory measures. Under the new law, organizations must take necessary measures to protect digital information that could be used to determine the identity of a user or that concerns a user's privacy.</p> <p>More information can be found at: http://www.china.org.cn/china/2012-12/28/content_27540911.htm</p>

Please note: The information provided above is strictly for educational purposes. It is not intended to be legal advice, either expressed or implied. Accurate Background recommends that you consult with your legal counsel regarding all employment regulations.

ANNUAL LEGAL UPDATE



Country / Jurisdiction	Bill / Statute Reference	Effective / Enacted Date	Impact	Description
Colombia	Statutory Law No. 1581 on Data Protection	Enacted October 17, 2012	Personal information, public records and verifications	Colombia has enacted an omnibus data protection law. It contains significant notice and consent requirements (e.g., express and informed consent prior to processing of personal data), European-style data subject rights, and cross-border data transfer restrictions, among other provisions. The law also calls for the establishment of a data protection authority. Organizations have a period of six months from the date of enactment before they must be compliant with the new law. More information can be found at: https://www.privacyassociation.org/media/pdf/knowledge_center/Colombian_DPA_Summary_2011_11.pdf
Ghana	Data Protection Bill	Passed February 10, 2012	Personal information, public records and verifications	After reports in July 2011 that the bill had been withdrawn from Ghana's Parliament for adjustments, it was re-introduced and passed by Parliament in February 2012. The Act, said to be awaiting presidential assent to be fully operational, is modeled upon European precedents and will set out the rights and responsibilities of data controllers, data processors and data subjects in relation to personal data, under the supervisory authority of a Data Protection Commission. More information can be found at: http://www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=229717
Hong Kong	Personal Data (Privacy) Ordinance (PDPO)	Passed June 27, 2012	Personal information, public records and verifications	The amendments to Hong Kong's data privacy regime came into force in July 2012, but they are being introduced in three phases. On October 1, 2012, rules on outsourcing personal data processing, disclosure of personal data without data user consent and a strengthening of the privacy commissioner's enforcement powers took effect. Phase two brings rules on direct marketing, while phase three will see the implementation of rules on legal assistance to "aggrieved individuals." More information can be found at: https://www.privacyassociation.org/publications/2012_09_01_hong_kong_amendments_to_hong_kong_personal_data_privacy_ordin

Please note: The information provided above is strictly for educational purposes. It is not intended to be legal advice, either expressed or implied. Accurate Background recommends that you consult with your legal counsel regarding all employment regulations.

ANNUAL LEGAL UPDATE

Country / Jurisdiction	Bill / Statute Reference	Effective / Enacted Date	Impact	Description
Hungary	Data Protection Act 2011	Passed April 18, 2011 Enacted January 1, 2012 Amended April 2, 2012	Personal information, public records and verifications	<p>The new law replaces Act LXIII of 1992 on the protection of Personal Data and Publication of the Data of Public Interest. It generally maintains the central provisions of the previous act, e.g., provisions on freedom of information. The subcontracting of data processing activities is still not allowed, and Binding Corporate Rules still do not form an adequate legal basis for international data transfers.</p> <p>The new law bolsters data protection enforcement by establishing a Data Protection Authority (DPA), which replaces the previous Data Commissioner.</p> <p>Because this bill was fiercely disputed, Hungary amended it in April 2012 to bring it in line with EU recommendations and strengthen the DPA agency's independence.</p>
Morocco	Act 09-08 on the Protection of Individuals with regard to Processing of Personal Data (Act 09-08)	Enacted February 23, 2009; Compliance required as of November 15, 2012	Privacy and personal information	<p>The new law, which has been gradually introduced over the past four years and is now enforced, aims to facilitate the growth of the digital economy while protecting privacy. It introduced a set of legal provisions aimed at protecting identity, rights and individual and collective freedoms as well as privacy against all attacks that may occur through use of computers. The law also establishes the National Personal Data Control and Protection Commission (or "CNDP"). The Commission is responsible for applying and ensuring compliance with the provisions of Act 09-08 and its implementing texts.</p> <p>Act 09-08 defines, inter alia, the right of access to databases containing personal information, the right to object to the processing of one's data, and the right to request correction of erroneous data and delete outdated information.</p> <p>More information can be found at: http://bakerxchange.com/rv/ff000c56b7edc537937637048244961954ffc4ad/p=1</p>

Please note: The information provided above is strictly for educational purposes. It is not intended to be legal advice, either expressed or implied. Accurate Background recommends that you consult with your legal counsel regarding all employment regulations.

ANNUAL LEGAL UPDATE



Country / Jurisdiction	Bill / Statute Reference	Effective / Enacted Date	Impact	Description
Netherlands	Amendment to Dutch Data Protection Act	Enacted February 9, 2012	Personal information	<p>Under the amended Data Protection Act, companies that use standard Contractual Clauses approved by the European Commission no longer require a permit for the transfer of personal data to countries outside of the European Economic Area (EEA). This is expected to reduce the administrative burden on these companies.</p> <p>Other changes to the Data Protection Act include higher fines for violations (from €7,600 to a maximum of €19,000 for failing to register the processing of personal data with the governing authority or intentional acts of omission), as well as additional obligations for the data controller.</p>
New Zealand	European Commission decision	Issued December 19, 2012	Personal information	<p>In December 2012, New Zealand became the latest country to qualify as meeting the EU adequacy standards for transferring personal data outside of the European Economic Area (EEA) for processing. The European Commission formally decided that New Zealand's Privacy Act 1993 offers an adequate level of data protection for the purposes of European law.</p> <p>More information can be found at: http://privacy.org.nz/european-union-endorses-new-zealand-privacy-act-media-release/</p>
Philippines	Data Privacy Act 2012 ("An Act Protecting Individual Information in Information and Communication Systems in the Government and the Private Sector.")	Passed by the Senate March 20, 2012; Signed by the president August 23, 2012	Personal information, public records and verifications	<p>The bill is based on the European Directive and is aligned with the Asia-Pacific Economic Cooperation Information Privacy Framework. This omnibus privacy legislation requires certain data security standards in addition to provisions on the handling of data by business process outsourcers (BPOs). The act establishes a National Privacy Commission in charge of implementation and enforcement.</p> <p>More information can be found at: http://manilastandardtoday.com/2012/08/29/bpo-companies-more-bullish-after-signing-of-data-privacy-law/</p>

Please note: The information provided above is strictly for educational purposes. It is not intended to be legal advice, either expressed or implied. Accurate Background recommends that you consult with your legal counsel regarding all employment regulations.

ANNUAL LEGAL UPDATE

Country / Jurisdiction	Bill / Statute Reference	Effective / Enacted Date	Impact	Description
Poland	Amended provisions of the Polish Data Protection Act 1997	Enacted January 1, 2012	Personal information	<p>The most significant changes to the act concern the provisions governing the transfer of personal data to third countries; i.e., outside the European Economic Area. Transfers of personal data to a third country may only occur if the country of destination ensures an adequate level of personal data protection.</p> <p>More information can be found at: https://www.privacyassociation.org/publications/2012_03_01_poland_reform_of_polish_data_protection_law</p>
Singapore	Personal Data Protection Act (PDPA)	Passed October 15, 2012 Expected to be enacted Q1 2013	Personal information, public records and verifications	<p>The PDPA establishes a mandatory data protection regime in Singapore. The new law seeks to undertake regulation in a manner that balances the right of individuals to protect their personal data against the legitimate need of organizations to collect, use or disclose personal data for business purposes. It prescribes the baseline data protection standards that apply to all private sector organizations in Singapore. The PDPA provides for a sunrise period of 18 months before the data protection requirements come into force.</p> <p>Organizations in certain industries (for example, banks, telecommunication service providers, healthcare institutions) will also face additional legal requirements specific to these industries.</p> <p>More information can be found at: http://www.singaporelawwatch.sg/slw/headlinesnews/18719-what-the-personal-data-protection-act-means.html</p>

Please note: The information provided above is strictly for educational purposes. It is not intended to be legal advice, either expressed or implied. Accurate Background recommends that you consult with your legal counsel regarding all employment regulations.

ANNUAL LEGAL UPDATE



Country / Jurisdiction	Bill / Statute Reference	Effective / Enacted Date	Impact	Description
Taiwan	Personal Data Protection Act (PDPA)	Effective October 1, 2012	Personal information, public records and verifications	<p>Taiwan has amended its data protection law; two controversial articles are still pending. The new law, known as the PDPA, broadens the definition of "personal data" and implements the following changes: (1) all enterprises and individuals that collect, process or use Personal Data are subject to the PDPA; (2) statutory requirements and procedures must be followed when collecting, processing or using Personal Data; (3) proper safety measures must be taken when retaining Personal Data files; (4) failure to comply with the PDPA will be subject to civil liabilities (up to NT\$200M), administrative penalties (up to NT\$500,000), and criminal liabilities (up to 5 years and/or NT\$1M).</p> <p>More information can be found at: http://www.bakermckenzie.com/files/Publication/65ed74cf-31e9-4df9-8a70-4f8e3b1c7319/Presentation/PublicationAttachment/1dd897f3-8929-4ef3-bf84-54efe8bea504/al_taiwan_pdpaeffective_oct12.pdf</p>
Ukraine	Amendments to the Law on Personal Data Protection	Effective December 20, 2012	Personal information, public records and verifications	<p>The main changes to the law are as follows: new grounds for the processing of personal data as an alternative to the individual's consent (e.g., the need to protect legitimate interests of data controllers or third parties); modified consent requirements; expanded rights of data subjects (e.g., the right to incorporate certain reservations/limitations into the consent, or revoke the consent); cancelled requirements to register employees' databases; treatment of personal data relating to public officers as "restricted information"; and exemption of journalists' professional activities. Additionally, the amended law imposes a set of adequacy requirements and conditions for cross-border data transfers.</p> <p>More information can be found at: http://www.lexology.com/library/detail.aspx?g=4e84948d-cc78-488b-963f-4410ba9e81f8</p>

Please note: The information provided above is strictly for educational purposes. It is not intended to be legal advice, either expressed or implied. Accurate Background recommends that you consult with your legal counsel regarding all employment regulations.

ANNUAL LEGAL UPDATE

Country / Jurisdiction	Bill / Statute Reference	Effective / Enacted Date	Impact	Description
Uruguay	European Commission decision	Issued August 21, 2012	Personal information	<p>In 2012, the European Union confirmed that Uruguay has achieved adequacy for personal data protection according to the standards of the EU Directive. This recognition implies an approval of the legal safeguards provided by Uruguay, which facilitates the flow and processing of personal data transferred to Uruguay from the EEA.</p> <p>More information can be found at: http://privacyconference2012.org/english/sobre-la-conferencia/noticias/Uruguay-logra-adequacion-en-Proteccion-de-datos-1</p>
Vietnam	new Labor Code	Passed June 18, 2012 Effective May 1, 2013	Personal information, verifications, health screening	<p>The new Labor Code requires both employees and employers to disclose certain kinds of relevant information during the hiring process. For example, employers must provide to employees information on social insurance, health insurance, salary, and other issues relating to labor contracts "that employees may want to know," and employees must disclose to employers "age, education background, qualification, health conditions and other issues that the employers may want to know." (Article 21)</p> <p>More information can be found at: http://www.lexology.com/library/detail.aspx?g=c2c953f5-ce51-4f3f-92ab-c29e53499d8f</p>

Please note: The information provided above is strictly for educational purposes. It is not intended to be legal advice, either expressed or implied. Accurate Background recommends that you consult with your legal counsel regarding all employment regulations.