Global HR Lawyers
Ius Laboris

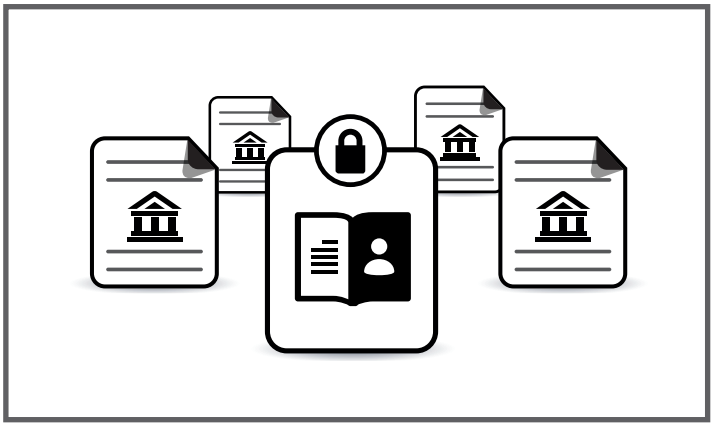
Inside

- Laws & regulations
- Employee recruitment
- Monitoring at work
- Employee personal devices
- 3rd party data transfers
- Consequences of breach

Data privacy in the Americas

At a glance

Laws & regulations



ARGENTINA

Act 25.326 regulates personal data protection and provides sanctions for improper use. Act 26.388 modified the criminal code to include improperly accessing/using protected data as a criminal act.

BRAZIL

Brazil does not have a comprehensive data protection framework, but the protection of privacy and personal information is considered a fundamental right. In general, the collection, record, access, transfer and use of personal information depend on the data subject's prior and express consent.

CANADA

Protections for federally regulated employees' information are set out in the Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA sets out general principles for the collection, use and disclosure of personal information. Private sector privacy legislation only exists in British Columbia, Alberta and Quebec. These Acts are substantially similar to PIPEDA. In the remaining provinces and territories, an employee's personal information is protected under the common law.

COLOMBIA

The protection of employees' personal data is governed by the general personal data processing laws: Law 1581 (2012), Decree 1377 (2013), and Decree 886 (2014) the General Data Protection Regime (GDPR).

MEXICO

The Mexican Constitution, the 2010 Federal Law on the Protection of Personal Data held by Private Parties, the 2011 Regulations of the Federal Law on the Protection of Personal Data held by Private Parties, the 2013 Guidelines of the Privacy Notice, the 2014 Parameters of Self-Regulation (the "Law") and the 2003 Federal Law to Prevent and Avoid Discrimination (Non Discrimination Law).

PANAMA

Article 29 of the Political Constitution of Panama stipulates that private mail and documents are inviolable and cannot be examined or held without an order issued by a competent authority for specific purposes, in accordance with legal formalities. In every case, the authorities will maintain the confidentiality over the private matters that were examined or held.

PERU

The Privacy Data Act (July, 4, 2011) and its Regulation (March 22, 2013) are Peru's data privacy laws; both apply to personal data in general, and not specifically to employees.

UNITED STATES

There is no single, comprehensive federal law regulating the collection and use of personal data. Instead, there are a number of federal and state laws and regulations that overlap and often contradict one another.

Some of the most prominent federal privacy laws include: The Federal Trade Commission Act (FTC Act); the Fair Credit Reporting Act (FCRA) the Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act Omnibus Rule (HIPAA/HITECH Act).

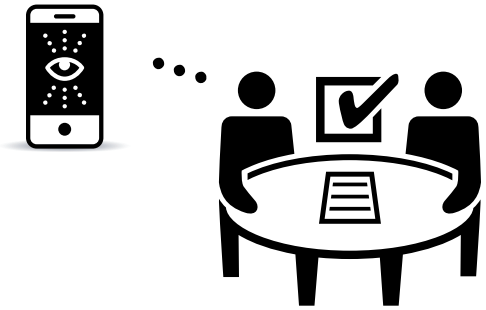
Currently 47 states, as well as the District of Columbia, Puerto Rico and the US Virgin Islands have enacted laws requiring notification of security breaches involving personal information. At least 29 states have enacted laws that require entities to destroy, dispose, or otherwise make personal information unreadable or undecipherable.

VENEZUELA

There is no specific law regarding data protection. Consequently, the matter has been regulated by rulings from the Supreme Court. The main criterion to determine if information amounts to personal data is whether the person submitting the data is identified, or can be identified based on said information.

The Supreme Court has declared that it is prohibited to use personal information for discriminatory purposes and creating a personal profile.

Employee recruitment



ARGENTINA

Employers are allowed to conduct background checks with some restrictions. An employer should not inquire about sexual preference, political opinions or religion. A candidate's criminal history can only be requested by public offices, courts or the employee. Medical examinations can be conducted, but certain tests require employee authorization.

BRAZIL

Applicable law imposes an express consent requirement through which users must opt in to have their data collected, stored and transferred.

Currently there is no express requirement for written permission as consent can be given in writing or by any other means that certifies it. The consent must be given separately from other contractual clauses.

CANADA

Consent to the collection of personal information can be express or implied from the circumstances. The nature or formality of consent depends upon the sensitivity of the information collected.

Under the Principles set out under the Federal PIPEDA, the completion of an employment application can be considered as consent to the collection of personal information.

British Colombia, Alberta and Quebec all have provincial Personal Information Protection Acts with varying requirements.

COLOMBIA

The GDPR imposes a general condition for Data Controllers to obtain the prior, express and informed consent from the data subjects at the moment of collecting personal data. If during recruitment, the employer wishes to obtain personal information from the candidate, such collection and further processing must comply with the "prior, express and informed consent" requirement. This requirement includes, but is not limited to, any "sensitive personal data" to be gathered by the employer.

MEXICO

All processing of personal data must be carried out in accordance with the Mexico's data protection principles. Additionally, employers must be careful not to discriminate during the recruitment process.

All data subjects must be given a privacy notice explaining the parameters of the collection of data and must give consent prior to the processing of their personal data. For sensitive data, explicit written consent is required. No consent is need when the collection of data is to fulfill employment obligations.

PANAMA

The Labor Code states that an employer may request a medical examination from a job applicant to ensure that the employee does not use illegal drugs or suffer from a mental illness that could create a risk for the employer or other employees. Job applicants must comply with this request.

Employers are limited by data protection laws and must not ask for an employee's confidential information without previous consent.

PERU

The processing of personal data shall be done with respect to the guiding principles of the Privacy Data Act. Thus, data must be processed adequately, for a particular purpose, after getting the consent of the data subject.

Accessing personal data available from public sources is not prohibited. However, the use and processing of the information obtained from public sources requires prior consent.

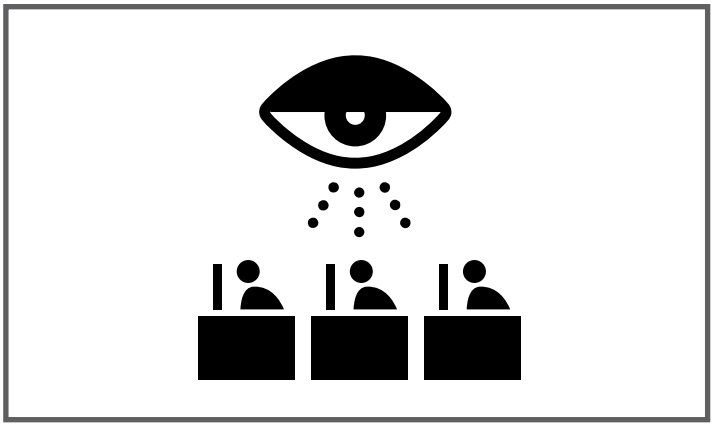
UNITED STATES

Nationally, 17 states and over 100 cities and counties have adopted laws, commonly known as "ban the box" laws, which prohibit employers from asking about a job candidate's conviction record during the application and interview process. Ten states limit employers' use of credit information in employment decisions.

VENEZUELA

Personal data can only be processed following certain data protection principles according to which the candidate must grant his consent and know what data has been collected, the purpose for collection, the users of the data, and be able to request the correction of erroneous or incomplete/excessive data. Personal data may only be preserved until the objective for which it was collected has been satisfied.

Monitoring at work



ARGENTINA

An employee's e-mails and internet activity can only be monitored with the employee's written consent. Under no circumstances can an employer monitor an employee's private email account.

BRAZIL

Surveillance of an employee's data at work is not regulated under Brazilian law. It is generally accepted that companies can monitor corporate e-mails and access to the web provided that (i) there is a written internal policy limiting private use (ii) monitoring is limited to protecting the company's property (iii) it does not breach the employee's privacy (iv) there are extraordinary circumstances to justify complete surveillance (v) confidentiality, protection and proper use of data is maintained (vi) an employee's private e-mail accounts are off-limits.

CANADA

There is an expectation of privacy in an employee's information created or communicated on an employer's device; this expectation can be displaced by explicitly putting an employee on notice that all information on the employer's devices, including personal information, may be accessed, surveilled, monitored or reviewed by the employer.

COLOMBIA

The courts maintain that, particularly in the workplace, employees have a reasonable expectation of privacy that needs to be protected even when the interests of the corporation are at stake. There are no concrete rules to follow when an employer's plans and policies involve the eventual intervention into an employee's data at work or on an employer's device, which is why many companies follow the general structure of the GDPR to reduce employees' expectation of privacy.

MEXICO

In all processing of personal data there is an expectation of privacy unless an employee is correctly informed that communications (including private communications), work tools or company owned property will be monitored and there is a reasonable justification for the monitoring. However, if the communications are marked as private, the employer must avoid opening them when possible.

PANAMA

Surveillance of employees' PCs and personal devices used for their work is permitted to prevent the use of these devices for personal purposes. However, access to employees' private data is not permitted.

PERU

Personal data can only be processed with prior consent that must be free, informed, express and unequivocal. Therefore, the access, use and transfer of employee´s information for purposes of surveillance/monitoring can only be carried out after getting prior consent from the employee.

UNITED STATES

Most employers have policies in their handbooks stating that employees have no expectation of privacy while using company owned computers and other electronic equipment. The bottom line is that if the employer owns the system, hardware or both, the employer can monitor employees' use of it, including personal files and communications.

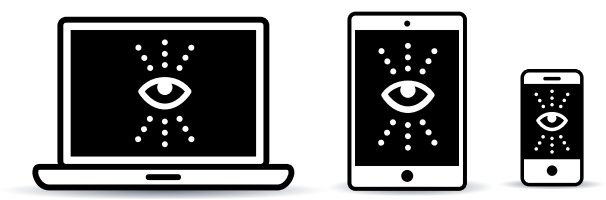
The National Labor Relations Board has held that employees generally have a right to use the employer's e-mail system during non-working time for organizing purposes, if the employer has allowed them to use the system for other non-work-related purposes.

VENEZUELA

All personal letters and e-mails are confidential, and therefore cannot be used in a Court without the consent of both the sender and the receiver. Monitoring an employee's personal data at work or on an employer's device must comply with the data protection principles.

Any work-related data can be monitored by the employer and used in Court by either the employee or the employer. The ownership of a device is not a criterion for whether data is protected.

Employee personal devices



ARGENTINA

Personal devices can only be monitored if there is a written policy that allows employees to work with their own device.

BRAZIL

While companies have the right to monitor the flow of data through corporate devices, the current position of the labor courts is that an employee's personal devices are entitled to privacy rights. Therefore, a company needs an employee's consent to access and monitor personal devices.

CANADA

An employer, as a condition of permitting access to an employer's data and systems, may put an employee on notice it has the right to access, monitor and manage all information on a personal device, which may include personal information, and which right includes the ability to transfer or delete data.

COLOMBIA

The law does not make a difference when the monitoring or inspection activities are performed on personal devices or on a company's machine. The Data Protection Agency has not issued any specific rules for monitoring these types of activities.

MEXICO

Employers cannot access the information contained in employee's personal devices without their informed, free and explicit consent even if the company's information may be stored in such devices. It is possible, however, for a company to monitor its internet or network following the principles provided for in the law.

PANAMA

Surveillance/monitoring of employment related data on personal devices requires previous authorization from the employee.

PERU

Personal data can only be processed with prior consent that must be free, informed, express and unequivocal. Therefore, the access, use and transfer of employee´s information for purposes of surveillance/monitoring can only be carried out after getting prior consent from the employee.

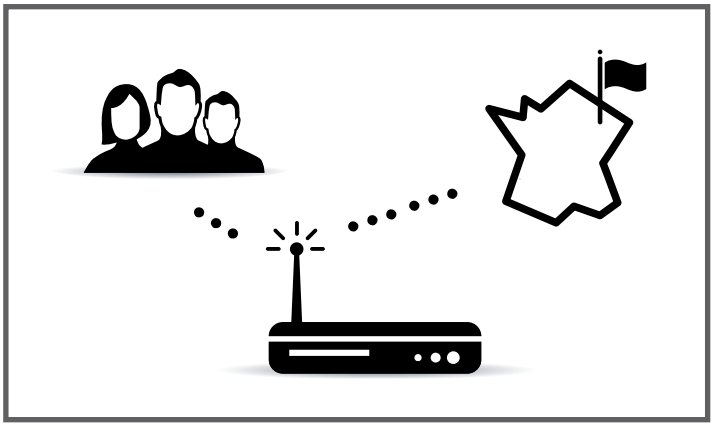
UNITED STATES

Generally, if the employee owns the device, the employer cannot monitor the files or communications. However, if the employee connects the device at work and the employer backs up its files, the employee's personal information may become part of the employer's system and then the employer can monitor the information. Employers who use remote wiping technology to remove company data from an employee's personal device after the employee changes employment may be subject to a lawsuit under the Computer Fraud and Abuse Act (CFAA), the Stored Communications Act, or state law, if the remote wiping deletes the employee's personal information, contacts, records, photos, etc.

VENEZUELA

If an employee uses a personal device for work-related purposes, the work-related data on the device is not protected.

3rd party data transfers



ARGENTINA

If the information is work related and the employees are informed, the information can be stored with a vendor inside or outside of the country. The employer must appoint an officer responsible for administrating the information.

BRAZIL

Brazilian law does not prevent companies from transferring national personal data to another country. However, pursuant to the Internet Law the transfer of personal data to a third party is subject to the data subject's prior and express consent.

CANADA

If the purpose of the movement of the data is for processing or purposes consistent with the reasons the information was first collected there are few restrictions on the transfer of data. Generally, such a movement of data is not considered to be a disclosure, but is a use, and the transferee will be considered to be the employer's agent.

Alberta's and Quebec's privacy acts provide differing requirements for the movement of personal data to a 3rd party.

In all transfers the employer remains responsible for the data transferred.

COLOMBIA

According to the principle of Restricted Circulation, personal data may only be shared with those persons that were authorized by the data subject. Therefore, personal data may circulate within a company only between those whose functions involve the processing of the data. Any transfer to third parties, even if to affiliated companies, must be previously authorized by the employee through express and informed consent; this principle is even stronger if the data is going to be sent abroad.

MEXICO

There are no restrictions based on location or 'adequacy finding' but data transfer agreements or data processing agreements must be executed between transferor and transferee, and the privacy notice that was made available to data subjects must be communicated to the transferee.

Consent for the transfer of personal data from controller to controller is required unless one of the exceptions provided for in the law applies.

PANAMA

Movement of personal data to a 3rd party requires the previous consent from the employee.

PERU

Any cross-border flow of personal data should be performed only if the country of destination maintains the same level of protection as that provided under Peru's Data Privacy Act and its regulation.

Any transfer of personal data requires the data subject´s consent, and should be limited to the same purpose upon which the personal information was provided. However, if the transfer of data is necessary for the execution of a contract to which the data subject is a party, consent is not necessary.

UNITED STATES

The United States has no single data protection law comparable to the EU's Data Protection Directive.

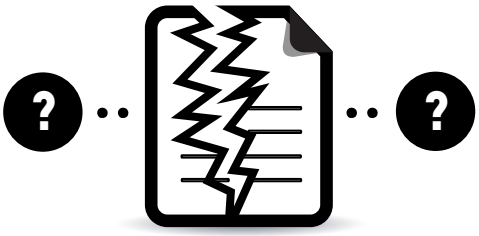
VENEZUELA

Personal data cannot be shared with third parties without the employee's previous, unambiguous, freely given, specific and informed consent.

Case Law prohibits the passing of the data to countries that do not ensure a level of protection for the rights and freedoms of data subjects that is in accordance with the data protection principles. However, there are no restrictions on transfers to any specific countries.

In any case, individual consent to transfer outside of Venezuela must be obtained. Given the low development of data protection rules in Venezuela, jurisdictions with moderate safeguards can be considered as offering an adequate level of protection.

Consequences of breach



ARGENTINA

Depending on the nature of the breach there could be criminal or civil sanctions including jail time (up to one year), an order to perform social work, administrative fines, damages and the closure of the data bank where the breach occurred.

BRAZIL

In case of a breach, an employee may be entitled to moral and material damages. Additionally, a company may be fined and/or ordered to adopt corrective measures or to cease its activities in Brazil.

CANADA

Under the federal PIPEDA, an employer may be ordered to correct its practices and/or pay damages, including damages for humiliation.

Under British Columbia and Alberta legislation, an employer may be ordered to change its practices, and an individual retains a cause of action in the courts for damages for actual harm.

Quebec's Private Sector Act, has a series of fines, based upon the seriousness of the breach, and an employer's prior convictions.

A change, though not yet in force, to PIPEDA will require notifying both the government and the individual of certain breaches.

COLOMBIA

The consequences for breach may include the imposition of (i) criminal penalties (ii) administrative fines/sanctions (iii) injunctive relief.

MEXICO

The consequences may include: (i) a warning (ii) the imposition of a fine ranging from 100 to 320,000 days of the General Current Minimum Wage in Mexico City (currently 70.29 Mexican pesos per day, during 2015). Fines may double when sensitive personal data is involved or in case of recidivism (iii) three months to five years of imprisonment for criminal acts with the possibility to double the time if sensitive personal data was involved.

PANAMA

Employees that are victims of data protection violations are entitled to claim material and moral damages, which may consist of monetary compensation, before a civil court.

PERU

In cases of breach, the Data Privacy Act sets forth administrative fines of up to approximately US$ 121,000.

UNITED STATES

Under the various data privacy laws in the US, penalties for breach can include: fines, injunctions, restitution to consumers, repayment of investigation and prosecution costs and imprisonment.

Additionally, Securities and Exchange Act regulations may require disclosure of breach, and board members may face personal liability. Shareholder derivative lawsuits are common.

VENEZUELA

Non-compliance with the principles stated in the Case Law can trigger civil lawsuits for habeas data, damages, and removal or correction of the collected data. In addition, the Case Law establishes that failure to comply with the data protection principles implies civil, administrative, and criminal liability.

Global HR Lawyers
Ius Laboris

The Americas

ARGENTINA

Funes de Rioja & Asociados

Av. Eduardo Madero 942
C1106ACW
Ciudad Autónoma de Buenos Aires, Argentina

T +54 11 43484100
E estudio@funes.com.ar

BRAZIL

Veirano Advogados

Av. Presidente Wilson, 231 23º floor
Rio de Janeiro
RJ 20030-021 Brazil

T +55 21 3824 4747
F +55 21 2262 4247
E contato@veirano.com.br

CANADA

Mathews Dinsdale & Clark LLP

RBC Centre, Suite 3600
155 Wellington Street West
Toronto, ON
M5V 3H1

T 416.862.8280
F 416.862.8247
E GMcGinnis@mathewsdinsdale.com

COLOMBIA

Brigard & Urrutia

Calle 70A N°. 4 - 41
Bogotá - Colombia

T +571 346 20 11
F +571 310 06 09 | +571 310 05 86
E servicioalcliente@bu.com.co
csantos@bu.com.co

MEXICO

Basham, Ringe y Correa S.C.

Paseo de los Tamarindos N°. 400 - A
Floor 9 Bosques de las Lomas
05120 México, D.F. Mexico

T +52 55 5261 0442
F +52 55 52 61 0496
E basham@basham.com.mx
jorgedepresno@basham.com.mx

PANAMA

Arosemena Noriega & Contreras

Tower Financial Center, 16th Floor
50th Street and Elvira Mendez
P.O. Box 0832-01091
Panama, Republic of Panama

T +507 366 8400
F +507 366 8457
E anc@anorco.com.pa

PERU

Estudio Olaechea

Bernardo Monteagudo 201, San Isidro
Lima 27, Peru

T +51 1 219-0400
F +51 1 219-0420 | +51 1 219 0422
E postmaster@esola.com.pe

UNITED STATES

FordHarrison

271 17th Street NW, Suite 1900
Atlanta, Georgia 30363
USA

T +1 404 888 3800
F +1 404 888 3863
E clientservice@fordharrison.com

VENEZUELA

D'Empaire Reyna Abogados

Edificio Bancaracas, P.H. Plaza La Castellana
1060 Venezuela

T +58 212 264.6244
F +58 212 264 7543
E VMarquez@dra.com.ve
ADisilvestro@dra.com.ve

Global HR Lawyers
Ius Laboris

280 Boulevard du Souverain – 1160 Brussels – Belgium
T +32 2 761 46 10 | F +32 2 761 45 15
info@iuslaboris.com – www.iuslaboris.com

Visit our innovative online platform providing international employers with a single point of reference for global HR law.

www.globalhrlaw.com