DATA PROTECTION & PRIVACY LAWS

Financier Worldwide canvasses the opinions of leading professionals around the world on the latest trends in data protection & privacy laws.
PAMELA GISHOLT
Associate
Arochi & Lindner Mexico
+52 55 4170 2123
pgisholt@arochilindner.com

Pamela Gisholt has worked as an associate in the intellectual property enforcement and information and communications technology departments of Arochi & Lindner Mexico since 2013. She has extensive experience protecting and enforcing the intellectual property rights of leading companies across several industries, including technology and electronics, entertainment and media, automotive, sports, fashion and luxury goods, and fast-moving consumer goods. Her practice focuses on developing and implementing strategies to protect and defend intellectual property rights, fight against piracy and counterfeiting, and comply with border measures, seizures and operations.

JOSE ANTONIO AROCHI
Head of ICT, InfoSec, Privacy and Media Department
Arochi & Lindner Mexico
+52 55 4170 2094
jarochi@arochilindner.com

José Antonio’s legal practice includes advising on strategies for the protection, compliance, defence and enforcement of intellectual property rights, mainly in the field of trademarks and patents. He is also an experienced counsellor in the field of information and communications technology, regulatory law, and advertising and marketing. His professional career encompasses three years working for an important intellectual property firm in Washington DC. This background allowed him to acquire an insight into the US legal system which, combined with his knowledge of the Mexican regulatory system, allows him to successfully advise national and international clients.
Q. Based on your experience, do companies in Mexico properly understand their data protection duties? To what extent are you seeing rising awareness?

A. In Mexico, personal data is a human right, and its protection is enshrined within a broad and robust legal framework. In the case of companies, the obligations they have toward personal data holders are established in the General Data Protection Law for the Public Sector, which has been in force since 2010. Due to the current and increased exposure of private personal information, data protection and corresponding enforcement activities have become stronger and gained ground; thus, although we have a long way to go, the business world has been pushed to focus on, accelerate its efforts toward and invest resources into personal data protection, to operate in accordance with the local legal framework. It is also important to consider that privacy compliance and data protection have become valuable assets for business competitiveness that allow companies to maintain, reinforce and increase their market share through customers’ trust.

Q. When companies undertake data processing activities – including handling, storage and transfer – what regulatory, financial and reputational risks do they need to manage?

A. Data privacy faces three main threats: data access illegitimacy, unauthorised data modification and data deletion. These threats can be defined as the combination of the possibility of a threat materialising and the negative consequences of the same. The continuous adoption of emerging data technologies has made data risk a pervasive concern for organisations, as data management implies several inherent and correlated risks which can impact a company’s reputation and thus its financial health. Considering the growing and continuous incorporation of technological mechanisms and resources, risks have increased in both type and impact. Some of the most common risks companies face are attacks and damage to their IT infrastructure, fraud, fines, legal claims, loss of business continuity and loss of brand value and reputation, which is directly related to the trust of individuals.
Q. What penalties might arise for a company that breaches or violates data or privacy laws in Mexico?

A. The data protection authority in Mexico is the Mexican Institute of Transparency and Personal Data Protection (INAI) and it is the entity in charge of transparency and access to public information, and personal data protection. The INAI is a constitutional and autonomous entity, empowered to enforce the law without meddling from other governmental entities. The INAI analyses each privacy matter when a claim is filed or a breach is detected. Sometimes the result of this analysis leads to the imposition of fines. For violations of privacy or data security law, the law provides a list of actions that are grounds for sanction. Fines range from 100 to 320,000 times the current minimum daily wage, or approximately US$5.38. In case of recurring infringements, an additional fine may be imposed and may be doubled when the case involves sensitive data. Sanctions may be imposed without prejudice to any civil or criminal liability that could arise.

Whether due to cyber attacks, systems glitches or human error, security breaches have been hugely impactful, creating both personal and social uncertainty.
Q. What insights can we draw from recent data breach cases? What impact have these events had on the data protection landscape?

A. Globally, personal data is becoming increasingly exposed, and Mexico is no exception. Whether due to cyber attacks, systems glitches or human error, security breaches have been hugely impactful, creating both personal and social uncertainty. Remote working is expected to become increasingly popular, gaining ground over traditional office work, which will also increase the chance of security breaches due to cyber attacks against employees in an effort to access company data, due to a lack of policies and training showing employees how to work remotely in a safe and correct manner, or due to a lack of technological and administrative security resources, among others. To minimise the cyber security gap, it is essential to raise awareness about the importance of implementing protection tools, since the ‘new normal’ has brought many opportunities, but also an increase in cyber security risks.

Q. In your experience, what steps should a company take to prepare for a potential data breach, such as developing response plans and understanding notification requirements?

A. A holistic data risk management system is the best way to be prepared for a potential data breach. However, there are some additional practices that could be implemented as part of a data breach prevention programme. As the knowledge, awareness and active participation of employees is essential in company operations and to correctly manage critical situations, the first step should be to implement a training and awareness programme which includes all employees, in addition to regular software updates and patches. In addition, regular risk assessments, encryption and data backups, as well as checklists to ensure that vendors and third-party partners maintain high data protection standards, are important. Companies should also conduct risk evaluations of third-party data security capabilities.
Q. What can companies do to manage internal risks and threats, such as rogue employees?

A. The ability to identify risks is a key part of strategic business planning as this will allow companies to take measures to control critical situations. Once risks have been identified, it is necessary to develop and implement administrative and technical tools. To comply with privacy and data protection legal frameworks, it is recommended that companies adopt privacy by design or privacy by default models. Implementing recruitment, selection and staff evaluation programmes that consider honesty, ethics and personal and professional integrity as elements of job performance, as well as continuously monitoring job satisfaction and the work environment, could help to detect red flags early. Awareness and staff training are essential. The use of antivirus and antispam software is essential. Data should be encrypted and strong passwords set and regularly updated. Companies must also manage user and access privileges.

Q. Going forward, how important will it be for companies to remain focused on data protection efforts, continually enhancing their controls and risk management processes?

A. The digital age has brought many benefits and challenges. Privacy and personal data processing have become important issues among users, consumers and businesses, due to the fact that the adoption of new technologies has raised potential risks for all parties involved. Therefore, both the public and private sectors have been pushed to strengthen regulatory frameworks, tools and mechanisms related to this matter, to protect the information managed by companies. The ability to protect personal data and to meet the security challenges of data processing with integrity are directly related to the trust of users and consumers, and therefore with the value and reputation of brands and companies in the market. That is why data protection and risk management programmes are not only a compliance endeavour but an essential part of business competitiveness.
Arochi & Lindner Mexico

www.arochilindner.com

AROCHI & LINDNER is a premier law firm with offices in Mexico and Spain and more than 25 years of experience providing world-class advice and representation in intellectual property, life sciences, advertising and marketing, civil and commercial dispute resolution, corporate, regulatory and data privacy law matters. The firm distinguishes itself with client-oriented service and an unwavering commitment to delivering results, efficiently and responsively, using its knowledge, experience and creativity. The firm tackles every matter with insight, savvy and an exceptional understanding of business needs.

JOSE ANTONIO AROCHI Head of ICT, InfoSec, Privacy and Media Department
+52 55 4170 2094
jarochi@arochilindner.com

PAMELA GISHOLT Associate
+52 55 4170 2123
pgisholt@arochilindner.com

VERÓNICA SITEN Privacy Consultant
+52 55 4170 2066
vsiten@arochilindner.com