DEUTSCH-BRASILIANISCHE INDUSTRIE- UND HANDELSKAMMER • VOL.3 • 2022

RECHT & STEUERN

NEWSLETTER

DE INTERNATIONAL

AHK MERCOSUL
Deutsch-Brasilianische Industrie- und Handelskammer
Câmara de Comércio e Indústria Brasil-Alemanha

EMDOC · Stüssi-Neves Advogados · Lefosse · Machado Associados · Taui Chequer Mayer Brown · Demarest

FCR Law / Fleury, Coimbra & Rhomberg Advogados · PN ST Pacheco Neto Sanden Teisseire Advogados · Sonia Marques Döbler Advogados · Rödl & Partner · Sperling Advogados

The potential threats of data breaches: Is it worth taking the risk?

Beatriz Graziano Chow
Associate Lawyer
bchow@sperling.adv.br
T (+55) 11 3704-0788

Lídia Alves Lage
Associate Lawyer
llage@sperling.adv.br
T (+55) 11 3704-0788

Sperling Advogados
Av. 9 de Julho, 4.939, 6º andar
Torre Jardim – 01407-200
Jardim Paulista – São Paulo/SP
T (+55) 11 3704 0788
www.sperling.adv.br

Sperling Advogados

The enactment of the Brazilian General Data Protection Law ("LGPD" in the Portuguese acronym) has drawn the attention of companies to a relevant matter: the need to put in place a secure environment for processing personal data. Such a safe environment, in a nutshell, depends on technical and governance measures related to information security, incident handling, and accountability towards data subjects to mitigate the multidimensional impacts that data breaches can have on a company's business.

Data breaches can quickly turn into public relations crises. They can yield reputational damage and loss of confidence in the market (blocking business opportunities). They can produce burdensome, lengthy administrative and judicial proceedings that culminate with the imposition of fines and sanctions that might harm shareholders, workers, and other relevant stakeholders. They can even generate contractual disputes with vital commercial partners with whom a company might share contractual obligations concerning data processing.

The LGPD establishes an obligation of both the controller and the processor to keep records of personal data processed in Brazil and invest in information security to guarantee its safeguard. According to the LGPD regime, the controller shall report a data breach if it results in significant risk or damage to the data subjects. The LGPD is silent, but a good practice is to enshrine in a controller/processor contract the obligation for the processor to notify the controller of any incident in due time.

The Brazilian Data Protection Authority ("ANPD") still has to regulate the minimum standards for processing agents to secure personal data. At this point, it is possible to say that ANPD is likely to adopt secondary regulation that is flexible enough in terms of technical standards and governance arrangements aimed to prevent, mitigate, and remediate risks inherent to information security. It doesn't mean "carte blanche" for controllers and processors. It just means that if data processing agents follow widely available and recognized best practices, enforcement measures by the regulator might be more nuanced instead of heavy-handed.

Although ransomware attacks have gained prominence in news headlines in the past few years, data breaches occur in several other forms, including acci-

Sperling Advogados
Av. 9 de Julho, 4.939, 6º andar
Torre Jardim – 01407-200
Jardim Paulista – São Paulo/SP
T (+55) 11 3704 0788
www.sperling.adv.br

dents and mistakes. For instance, an employee who sends confidential information to a client that was not supposed to come in contact with a specific dataset, or a person who inadvertently leaves a device filled with personal data unattended and the device does not count on the appropriate safety and security measures. In cases like that, it is not easy to assign responsibility for an incident (as it is not uncommon that beyond personal negligence or malpractice, more structural flaws in information security practices and data handling governance schemes are the ones to blame).

Acquiring an adequate level of protection for data and information security are processes with no endpoint. They are permanent and incremental processes. Besides regulatory guidance (as regulation is not only about sanctioning) and obligations, data protection also depends on adopting internationally recognized standards, codes of conduct, and corporate policies (including voluntarily). It also can gain a lot from multistakeholder dialogues, sharing best practices, and learning by doing.

In Brazil, there are challenges for companies to reach higher maturity levels regarding information security and readiness for incident handling. The ANPD is still in its early years of institutional development and might have been unable so far to provide concrete guidance as fast as the market requires (despite all the efforts and excellent work that the Authority has done so far on multiple other fronts). Also, the cost of implementing high-end data protection programs can be significantly high, especially for small and medium businesses. As organizations change at a dynamic pace (and technology is developing even faster), keeping up with high standards for information security and operational excellence in incident handling, in the long run, is also challenging. On top of that, there is also the challenge of creating a data protection culture across the board in complex corporate settings, let alone in society.

Despite those challenges, we believe that organizations should evolve and invest in a combination of controls, governance, and technologies to protect their underlying IT systems and data handling processes, even if, in the short term, they may represent the reduction of profit margins or revenue loss. In the long run, however, we are confident that investments in those areas will payoff for three reasons: First, they represent ways of closing the doors to hacking, computer fraud, and other malicious activities (in 2021 alone, Brazil suffered more than 88.5 billion attempts of cyberattacks, according to the Fortinet[1] report). Second, they can contribute to enhancing operational excellence and reducing or minimizing other sorts of security incidents. Third, all

[1] Available at: <https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021>.

Deutsch-Brasilianische Industrie- und Handelskammer São Paulo

Rua Verbo Divino, 1488 - 3º andar
04719-904 São Paulo - SP - Brasilien
T (0055 11) 5187-5216
F (0055 11) 5181-7013
E juridico@ahkbrasil.com

www.ahkbrasil.com