June 4, 2020

# Data Privacy Concerns for Latin American Businesses During COVID-19

**Attorneys**
Edward R. McNicholas
Nicholas M. Berg
María González Calvet
Danielle Bogaards
Nataša Siveski

Data privacy concerns have played an increasing role in the way companies handle anti-corruption investigations, particularly as they relate to obligations to foreign enforcement authorities. In-house counsel and compliance professionals must continue to be mindful of national data privacy obligations while ensuring full cooperation with investigating authorities. And as more Latin American businesses have been forced to work remotely during the COVID-19 pandemic, data privacy concerns have come to the forefront as businesses adapt and a new way of attacks target the now dispersed workforce.

Remote work also brings to light fundamental oversight concerns, both of a company's internal processes and procedures, and in the context of maintaining a robust third party management system. Setting the appropriate tone from the top that gatekeeping functions cannot falter will ensure that employees working remotely do not take shortcuts and continue to comply with their obligations.

## Evolution of Data Privacy Laws in Latin America

By way of background, data privacy regulations in Latin America find their origins in the concept of *Habeas Data*, which grants a right to privacy as a safeguard of personal dignity—including protection of an individual's image, privacy, honor, self-determination of information and the freedom of information of a person. The notion of habeas data is grounded in various countries' constitutions, allowing citizens the right to demand access to, object to, or correct processing of their personal information. For example, Mexico and Columbia's Constitutions afford citizens the right to privacy, and the Argentine Constitution specifically affords individuals the right to obtain information pertaining to themselves that is registered in public or private databases. But while individuals are given agency to protect their own privacy rights, habeas data alone does not require data processors to ensure the protection or privacy of personal data.

As recently as a few years ago, the lack of specific measures for data processors to safeguard personal data against cybersecurity breaches culminated in two notable breaches, changing the way Latin American countries view data protection and security. The Panama Papers and Paradise Papers became international scandals, as millions of documents were leaked from law firms and service providers, disclosing financial information of high net-worth individuals or companies and revealing occasions of money laundering and "tax engineering."[1] With the uncovered treasure trove of documents implicating global companies across all industries, enforcement authorities were effectively given a 'follow-the-money' road map to launch a significant number of corruption investigations. The investigations led to significant cooperation among foreign enforcement agencies.

[1] Nick Hopkins and Helena Bengtsson, *What are the Paradise Papers and what do they tell us?*, THE GUARDIAN (Nov. 5, 2017), *available at* theguardian.com/news/2017/nov/05/what-are-the-paradise-papers-and-what-do-they-tell-us; see also Luke Harding, *What are the Panama Papers? A guide to history's biggest data leak*, THE GUARDIAN (Apr. 5, 2016), *available at* https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers.

In the aftermath of these high profile data breaches, many Latin American countries have worked to improve their data privacy regulations, increasing their cyber security efforts to protect personal data. During this time, the European Union established the General Data Protection Regulation ("GDPR").[2] The GDPR is widely renowned for its high standard of the treatment of personal data, containing broad provisions related to the protection of personal data and privacy. Various countries have adopted the GDPR to become part of an international data privacy framework, largely due to its application to companies located in the EU that process personal data, but also on companies outside the EU that process personal data of EU citizens.

Latin American neo-nationalist critics, however, have opposed adopting a united international common policy, favoring instead the development of their own approach to cybersecurity measures. So, rather than adopting the GDPR directly, Latin American countries have looked to it an example to update their individual data privacy legislations. For example, Argentina proposed a bill in 2018 that aligns with the GDPR, Brazil has worked to consolidate the over 40 Brazilian data privacy regulations into the Lei Geral De Protecao de Dados ("LGPD") which also mirrors the GDPR (though implementation has been postponed to May 2021 due to COVID-19),[3] while Chile, Mexico and Uruguay also taking steps in reforming their existing data privacy laws to increase privacy and security protections outlined in the GDPR.

These restrictive data privacy laws have significantly impacted the way companies approach internal investigations. It can be difficult for companies trying to navigate cooperation with broad and many times heavy-handed EU and U.S. governmental inquiries, while simultaneously protecting against the unnecessary disclosure of personal information and ensuring compliance with local data privacy laws.

## Data Privacy Concerns for Latin American Businesses Working Remotely During Covid-19

Awareness of the various data privacy standards throughout Latin America is increasingly important because the way data is handled continues to evolve in the current COVID-19 climate. For example, the Chilean data privacy oversight committee (Council for Transparency ("CLPT")) is looking for ways to narrow a congressional data protection bill that authorizes transfers of personal data between governmental bodies, such as adding security measures to anonymize citizen's sensitive health data when monitoring citizen's geolocation data to combat COVID-19, and limit the time period for sharing sensitive data through the various state-run bodies.[4] Brazil has postponed the implementation of the LGPD from August 2020 to May 2021,[5] and the Brazilian Supreme Court addressed data privacy for the first time, suspending the president's provisional measure MP 954/2020 that would have required telecommunication companies to share their database with a Brazilian research institute during the pandemic, in part because the provision would expose citizen's

[2] Regulation (EU) 2016/679.
[3] *Brazil: President promulgates provisional measure postponing LGPD to May 2021*, DataGuidance (Apr. 30, 2020), https://www.dataguidance.com/news/brazil-president-promulgates-provisional-measure-postponing-lgpd-may-2021?dm_i=437F,14M2Q,62IFIK,3Z29E,1.
[4] Caio Rinaldi, *Chilean Council for Transparency Seeks Changes to Coronavirus-Related Data Protection Bill*, MLex Market Insight (May 8, 2020).
[5] *Brazil: President promulgates provisional measure postponing LGPD to May 2021*, DataGuidance (Apr. 30, 2020), https://www.dataguidance.com/news/brazil-president-promulgates-provisional-measure-postponing-lgpd-may-2021?dm_i=437F,14M2Q,62IFIK,3Z29E,1.

private information when the scope of information collected was not sufficiently limited, and the text did not include security mechanisms to protect consumers' data.[6]

The following categories address key data privacy concerns employers may consider: (1) protecting information from hackers when data is processed in less secure remote environments, (2) oversight of data shared amongst third parties and telecommunications companies, and (3) oversight of employee's actions as they work remotely.

## Protect Information from Hyper-Active Hackers

The COVID-19 pandemic has required more employees to work remotely, which translates to data being taken away from an office setting and placing company data in the homes of preoccupied employees. Further, in an increasingly global and interconnected world, the vast majority of organizations and businesses rely, at least to some extent, on IT systems and services provided by third parties. Hackers will look for weaknesses in the expansion of at-home access points.

Best practices for working remotely involves both updated security policies, employee training, and a plan in place should a breach occur:

- ***Focus on ways to safeguard the security of their IT systems.*** For example, among other things, businesses should ensure employees are able to use secure networks and not public Wi-Fi, access systems only through VPNs, use multi-factor authentication at all log-in instances, and timely encryption and software patching and updates.
- ***Educate employees.*** Employees should be reminded of the importance of confidentiality and organizations should ensure that appropriate data security policies are in place and adhered to. For example, acceptable use and 'bring your own device' policies, as well as the procedures to be followed if they suspect a data breach occurred. Further, employees adjusting to this "new normal" may be less attentive to cyber threats, so businesses should remind employees how to identify COVID-19 related phishing emails that exhibit increasing sophistication.
- ***Have a data security breach response plan.*** If a breach occurs, companies should have a plan in place on how to manage the situation, including who within the organization will handle the breach, forensic investigation and reporting. Latin American countries are not consistent in their breach notification requirements—for example, Argentina and Chile do not have a notice requirement, but Brazil and Mexico require the data controller to report an incident to relevant authorities and/or the individual's whose data was breached. This inconsistency in reporting makes it important for companies, particularly international companies, to be familiar with notification laws relevant in their country, and countries of individuals whose data the company processes.

## Ensuring Proper Oversight of Third Parties

Additionally, conducting "business as usual" may not be possible in industries considered at a high risk for corruption, where significant interactions with third parties are required, and where operations are global and encompass high risk

[6] Ana Paula Candil, *Comment: Brazilian Supreme Court Addresses Data Privacy for First Time in Statistics-Collection Case*, MLex Market Insight (May 8, 2020).

regions. Significantly, employees in compliance functions, who are now working from home and restricted from traveling, are expected to continue to perform at a high level and oversee the riskiest aspects of their organizations remotely. Where they would previously visit sites as part of their third party due diligence or conduct on-the-ground audits of international subsidiaries, suppliers, and potential business partners, compliance personnel must endeavor to mitigate risks remotely, treading cautiously to simultaneously ensure data privacy laws are not infringed. Remote also requires cooperation from counterparties who may not be compelled to promptly provide relevant materials or do not have the information technology infrastructure to facilitate large or secure data transfers.

Best practices for ensuring robust remote oversight involves an action plan, communication plan, and survey on relevant laws.

- ***Collaborate on action plan with employees.*** In-house counsel overseeing compliance areas should endeavor to come up with a streamlined action plan and checklists for the oversight of subsidiaries and third parties to ensure tasks are completed, taking into consideration the remote work capabilities of personnel.
- ***Communicate with subsidiaries and third parties.*** In-house counsel should send official communications to subsidiaries and third parties to lay out expectations for cooperation.
- ***Conduct data privacy laws survey.*** To the extent employees are seeking information remotely from new jurisdictions or requesting new information from familiar jurisdictions that may implicate data privacy laws, companies should endeavor to conduct a survey of relevant data privacy laws.

## Ensuring Proper Oversight of Employees

Further, with increased vulnerability and decreased internal oversight, companies have questioned whether they can monitor their employees who are working remotely due to COVID-19. For example, employers may have concerns in employee productivity and performance, and are unable to benefit from face-to-face monitoring an office environment allows. While technology providers may offer remote monitoring solutions, such as work device webcams and key stroke assessments, companies in countries with more robust data protection laws, such as those aligned with the GDPR, would be wise to consider the following data privacy concerns:

- ***Employee's Privacy Rights.*** As discussed in the beginning of this article, individuals have a fundamental right to privacy, especially in their home. One of the core elements of Latin America's privacy laws is the right of all individuals to access the information that organizations have collected about them and provide input on the accuracy of that information. As such, if a company monitors its remote employees, it should ensure employees are able to access what information was taken as part of the monitoring.
- ***Notice to Employees.*** As a best practice, companies should communicate with employees about their approach to their monitoring. Latin American countries' data privacy laws, while not uniform, generally include a notice obligation to individuals, informing them of what personal information is being collected, why, and with whom it is shared. Companies should employees are notified of the methods and scope of monitoring and personal information being processed.

- ***DPIAs.*** Conduct a formal data protection impact assessment ("DPIA") before implementing any form of employee monitoring, and safeguard information obtained through monitoring. The various data privacy laws in Latin America require organizations that collect, use and disclose personal information to take reasonable precautions to protect that information from loss, misuse and unauthorized access, disclosure, alteration and destruction.
- ***Legal Basis and Proportionality.*** Companies have a legitimate interest as a legal basis in processing personal data obtained through monitoring (e.g., to improve employee productivity or to ensure compliance with organizational policies). This means the company should ensure the benefits of monitoring outweigh the employee's reasonable right to privacy expectations and risk of harm, damage or distress, that the purpose of monitoring are sufficiently important and no more restrictive than necessary to achieve its goal. However, a word of caution: data controllers should be wary when toeing the line of justifiable monitoring, mindful that otherwise excessive measures--that are reasonable during a pandemic—do not become the new standard of data privacy regarding personal data.
- For more information on this subject, refer to the following Ropes & Gray client alert, here.

## Conclusion

Remote working during COVID-19 raises serious data privacy and anti-corruption issues, particularly concerning thorny areas in the context of internal investigation and responding to government inquiries include data processing, data collection, data transfer, and the mechanisms by which data is processed. It is critical for companies to develop strategies that have these concerns in mind, particularly where information sharing with international authorities is required, and privacy laws differ on a country-by-country basis.