LATAM COVID-19 Task Force – Privacy and Cybersecurity Issues

July 1, 2020

AUTHORS

Maria-Leticia Ossa Daza | Daniel K. Alvarez | Nicholas Chanin

Introduction

Governments and companies around the world continue to grapple with the changes brought on by the COVID-19 pandemic. While different countries are at different stages of dealing with the pandemic, one of the constants has been the number of important privacy and cybersecurity questions raised by response efforts. In a series of prior client alerts, we have already highlighted some of the key issues companies are wrestling with, and the guidance that has been provided by various governments and regulators in the United States, Canada, the United Kingdom, and the European Union.

In this Client Alert, we examine these questions as they relate to companies that operate in Latin America. Navigating the numerous country-by-country laws in this region can be a challenging exercise even under normal circumstances, and particularly so for companies that need to account for privacy and cybersecurity regimes in the United States, European Union, and other countries and regions. In collaboration with our colleagues at law firms throughout this region, we have compiled country-by-country insights, analyses, and information on the privacy and cybersecurity challenges that companies operating in Latin America face as a result of the COVID-19 pandemic–including some of the key questions raised by companies in each country, whether regulators have provided specific guidance, and how the COVID-19 pandemic has affected the applicable legal regime–as well as how companies are addressing these challenges.

Key Themes

A review of the information provided by our colleagues across this region reveals a handful of key themes for any companies operating in Latin America.

- **Your Security Approach Must Adapt to Changing Circumstances**

The COVID-19 pandemic has forced massive changes to most companies' risk profile by moving employees from a controlled office environment to remote work environments. As our colleagues from Chile have stated, "teleworking and remote meetings have become an everyday standard." This change has tremendous implications for companies' efforts to maintain the security and integrity of their data, networks, IT infrastructure, and other diligent assets. Regulators and other government agencies from the United States to Argentina have issued guidance to help companies identify and defend themselves against the increased risks associated with these changes. Companies that fail to take reasonable steps to identify how their risk profile has changed and to address those changes through new tools, training, or other tactics are likely to find themselves at increased risk of a successful attack by a malicious actor, as well as increased risk of legal liability from the government, consumers, and shareholders.

- **A Complex Web of Privacy and Security Laws Requires Attention to Detail**

Organizations operating across Latin American must navigate a complex web of privacy and data security laws to maintain compliance. That web becomes even more complex when factoring in compliance with the privacy and data security regimes in the U.S. and the EU. The COVID-19 pandemic has brought many of the differences between these laws into stark relief. For example, some jurisdictions' laws generally prohibit the collection of *any* health-related information about an individual without that individual's consent, but other jurisdictions do allow such collection without consent in certain circumstances and still other jurisdictions are actually requiring such collection as part of any re-opening efforts. With numerous governments across this region issuing country-specific guidance on COVID-related data collection efforts, it is more important than ever for companies to know what jurisdiction's laws apply to a particular piece of data, and to have systems, policies, and controls in place that allow for any differential treatment that may be required.

- **Health-Related Data Is Considered "Sensitive" Data Across this Region**

Most of the data that companies are likely to collect as a result of the COVID-19 pandemic—e.g., temperature checks, symptom and medical history, etc.—is likely to be considered "sensitive," health-related data in many jurisdictions, and as "sensitive" data it will likely be subject to more robust requirements around its collection, use, storage, sharing, and destruction. For example, laws and guidance from regulators in Colombia and Uruguay specifically highlight that health-related information is considered sensitive information and, as a result, requires affirmative consent from the individual before collection, use, or sharing, and requires heightened levels of security, etc. The same holds true for new laws that are soon to be in effect in Panama and Brazil, as well as in countries where privacy protections spring from the country's constitution rather than a specific statute or regulation. Companies that do not normally collect and use such data will want to ensure that their internal policies and controls are sufficiently robust in light of the requirements that attach to such data, and that any privacy policy or other notice provided to the individuals whose data is being collected satisfies any

legal requirements while giving the company sufficient flexibility to use the data for its stated purposes.

- **Stay Flexible**

The ultimate lesson of the experience that companies are having with the COVID-19 pandemic is to stay flexible and be prepared to adapt to changing circumstances. In various countries, including the United States, policy makers have pushed for changes to existing law specifically with respect to information collected in response to the COVID-19 pandemic. In other countries, most notably Brazil, policy makers are considering options to delay the implementation and enforcement of general privacy laws that were set to go into effect. Throughout this region, the pandemic has caused governments and policy makers to reconsider some of their basic assumptions about how privacy laws should work, particularly in light of the potentially critical role that data could play in helping to contain the COVID-19 pandemic. As governments, regulators, companies, and consumers learn more about the long-term effects of the COVID-19 pandemic and the data that is being collected, we are likely to continue to see changes to the laws and regulations that apply and how regulators and government policy makers apply them.

Questions

The questions and responses from the members of the LATAM COVID-19 Task Force have been organized in accordance with the categories below. Both the questions and the responses can be accessed by scrolling down to the relevant section of the memo or by selecting the title of each category below.[1]

1. **How should companies in your country think about privacy and cybersecurity issues in the context of COVID-19?**
2. **Has the relevant regulator(s) in your country issued any guidance, rulings, or other public statements about how companies should address privacy or cybersecurity issues raised by the COVID-19 pandemic?**
3. **Are there any changes to existing law that have been undertaken as a result of, indirectly or directly, the COVID-19 pandemic?**
4. **What are some of the key/repeat questions you have heard from clients trying to deal with the privacy and cybersecurity issues raised by COVID-19?**
5. **What do you anticipate the medium- and long-term effects of COVID-19 will be on privacy/cybersecurity issues? For example, do you think this will make it more/less likely that new legislation will be enacted related to privacy? Will it change how much and what kinds of information companies collect about their employees?**

Since we have asked the same questions about events and developments in multiple countries in this region, we hope that the collective feedback will provide some basis for comparison across this region and some insight into potentially developing trends in responses and actions.

[1] NOTE: The responses to these questions may include hyperlinks to certain websites that may be blocked by your company's network and may require that you access the link from a separate system.

Future Updates to this Client Alert

The LATAM COVID-19 Task Force plan to update the responses periodically to reflect the evolving situation. You can access all of Willkie's COVID-19 publications at our COVID-19 Resource Center.

Questions and Feedback

We look forward to having an active conversation with you and hearing about any concerns and questions you may have which you can direct to LATAMCovid19@willkie.com.

Maria-Leticia Ossa Daza

Daniel K. Alvarez

Nicholas Chanin

LATAM COVID-19 Task Force Members

The following law firms participated in this client alert of the LATAM COVID-19 Task Force:

Country	Law Firm	Point(s)-of-Contact
Argentina	Marval O'Farrell Mairal	Diego Fernández, Mariano J. Peruzzotti
Brazil	Lefosse Advogados	Paulo Lilla
Chile	Barros & Errázuriz	Andrés Rodríguez, Pablo Guerrero Valenzuela, Magdalena Rojas
Colombia	Brigard Urrutia	Juan Nicolás Laverde, Sergio Michelsen, Luis Felipe García Rubio
Costa Rica	BLP Legal	Julio Castellanos
Ecuador	Pérez Bustamante & Ponce	Camila Mateus

Mexico	Mijares, Angoitia, Cortés y Fuentes, S.C.	Gabriel Calvillo Díaz, Martín Sánchez Bretón, Patricio Trad Cepeda
Panama	Fabrega Molino	Mario Preciado, Denisse Correa
Peru	Rebaza, Alcázar & De Las Casas	Stefano Amprimo, Alexandra Orbezo, María del Pilar Sánchez
Spain	Pérez-Llorca	Andy Ramos Gil de la Haza, Andrea Sánchez
Uruguay	Guyer & Regules	Sofía Anza Guerra, Angeles Castaingdebat Castro, Corina Bove, Nicolás Piaggio, Cecilia Orlando
Venezuela	D'Empaire	José Valecillos, José Valentín González P., Daniel Bustos

PRIVACY AND CYBERSECURITY

1. How should companies in your country think about privacy and cybersecurity issues in the context of COVID-19?

Country	Answer
Argentina	In our opinion, companies should take necessary steps to ensure that all work is carried out on devices that have adequate security measures, especially when employees use their personal devices to perform work-related tasks. Work-related tasks from non-secure devices and networks should not be allowed. Moreover, it is important for companies to have appropriate privacy, acceptable use of information resources, and "bring your own device" internal policies; not only to establish how work tools should be used, but also to regulate the employee's expectation of privacy when performing their work-related tasks.
Brazil	The COVID-19 pandemic has created a new reality that companies have adapted to in order to maintain business continuity via technologies such as telecommuting. These changes impose considerable technical challenges, as the use of large-scale telecommuting can increase the companies' exposure to privacy, data protection, and security risks. Moreover, after the isolation measures end, companies will face new challenges, as they will be eager to carry out tests to check whether their employees and visitors have symptoms of COVID-19. This scenario also brings privacy and data protection concerns, especially in the context of processing of sensitive personal data, a category of personal data that includes information concerning health.[2] Concerns about such privacy and cybersecurity risks are even more relevant considering that the Brazilian General Data Protection Law (*Lei Geral de Proteção de Dados Pessoais* – "LGPD") will come into effect soon. Inspired by the EU's General Data Protection Regulation ("GDPR"), the LGPD defines a comprehensive set of rules that promises to reshape how companies, organizations and public authorities collect, use, process, and store personal data when carrying out their activities. The LGPD also requires data controllers and processors to adopt technical and administrative security measures to protect personal data from unauthorized access or any other form of unlawful processing. In any event, it is not clear at this point when the LGPD will be effective, as described in more detail below.
Chile	In the context of the COVID-19 pandemic, where teleworking and remote meetings have become an everyday standard, companies need to take all the necessary measures to prevent data breaches. We have seen how cybercriminals can easily access teleconferencing calls – where strategic information is being shared – when companies do not take all the necessary cybersecurity measures in order to avoid such exposures. The implementation of a remote working protocol, which was already being carried out only by some "innovative companies" before the disruption of COVID-19, has been dramatically accelerated and generalized by the pandemic, imposing new challenges to companies that need to adapt their data protection standards and cybersecurity measures to this new way of working. Accordingly, simple and clear teleworking policies could help employees and partners understand that working from home is not synonymous with relaxing security and data privacy standards.

[2] Sensitive data is defined as "personal data on racial or ethnic origin, religious belief, public opinion, affiliation to union or religious, philosophical or political organization, data relating to the health or sex life, genetic or biometric data, whenever related to a natural person" (Art. 5, II, of Law No. 13,709/18 - LGPD).

LATAM COVID-19 Task Force – Privacy and Cybersecurity Issues

Colombia	Companies in Colombia face a significant challenge in balancing their duties to best protect their workforce and the public at large (businesses have to implement health protocols to prevent the spread of COVID-19 when they resume activities), to continue to expand their operations amidst the COVID-19 crisis (i.e., through remote-work schemes), and to comply with local data protection laws (Law 1581 of 2012 and Decree 1074 of 2015). In the absence of specific and comprehensive guidance on the part of Colombian authorities, companies should take a proactive approach to best tackle privacy and cybersecurity issues in the context of COVID-19, while being mindful of the strong and permanent enforcement of privacy and data protection regulations by the *Superintendencia de Industria y Comercio*, the Colombian Data Protection Authority (the "SIC"). Health information is considered sensitive data under Colombian data protection laws (Law 1581 of 2012 and Decree 1074 of 2015). Processing sensitive data is generally prohibited, save, among other cases, when data subjects provide their prior, express and informed consent, and in cases of medical or sanitary urgency. The notion of "medical and sanitary urgency" provides legal grounds for companies to temporarily process health personal data to address, prevent, manage and/or control the spread of COVID-19 and mitigate its effects. Nevertheless, bearing in mind that sensitive data is subject to enhanced levels of protection, it is advisable that companies always (i) try to obtain consent from data subjects if possible; (ii) use information exclusively for purposes of preventing and managing risks related to COVID-19; (iii) keep information under security conditions to prevent its loss, alteration or unauthorized access, disclosure or use; and (iv) conduct a data protection impact assessment to keep, record, and seek an adequate balance between data processing operations, legal basis, and the proportionality and adequacy of measures implemented to keep data safe.
Costa Rica	Companies in Costa Rica should focus on the cybersecurity risks of having a significant number of their employees working from home. Also, sensitive information may be required in order to prevent employees or customers who are infected with COVID-19 from accessing companies' facilities. In Costa Rica, this would be a real challenge from a legal standpoint because sensitive personal data can only be collected and processed under limited exceptions.
Ecuador	Ecuador faces a big challenge in all legal matters related to privacy and cybersecurity. It's important to mention that despite the fact that privacy rights are recognized and guaranteed by the Ecuadorian Constitution as fundamental rights, the lack of specific privacy regulations and regulatory authorities has led to a social and corporate culture that does not respect or give much attention to these fundamental rights. However, now that we are going through a pandemic where companies **must** deal with additional personal sensitive information (e.g., medical information related to possible and confirmed cases of COVID-19) and corporate confidential information might be exposed to cybersecurity issues, companies must start considering privacy and cybersecurity matters seriously. We have been advising our clients since the beginning of the pandemic that all COVID-19-related information which is personal data must be treated according to certain regulations included in the Ecuadorian medical and commercial laws and the Ecuadorian Constitution. In our experience, bigger companies and multinationals are better prepared to deal with personal information obtained due to COVID-19 than small companies, which suffer from lack of knowledge, information and preparation. For further information, please refer to the links below: https://www.pbplaw.com/es/covid-19-la-importancia-de-los-datos-personales/ https://www.pbplaw.com/es/proteccion-de-datos-en-epoca-de-coronavirus/
Mexico	Recent federal and state guidelines issued by work and health federal authorities of the Mexican government intended to mitigate the risk of contagion of COVID-19 in the workplace, require private companies to collect specific data from employees that have tested positive for COVID-19, as well as employees that came into direct contact with infected employees. Companies should consider this data as sensitive information, and all databases containing any COVID-19 cases or related information should be handled in accordance with private data protection regulations, especially those restricting the transfer of data to any third parties.

Panama	Although Panama's first personal data protection law, Law No. 81 of 2019 on the Protection of Personal Data will not come into effect until March 2021, the concept of personal private communications and documents is already regulated in the Panamanian Constitution as a fundamental right (article 29), and the consent of the interested subject is required for the transfer of any personal information (article 42). Furthermore, Law 68 of 2003 regulates the information and confidentiality rights of patients. Likewise, every person has the right to confidential medical records. Any company who fails to comply with these regulations may be subject to severe sanctions pursuant to the Penal Code. In light of the above, even though Law No. 81 of 2019 has not yet entered into effect, companies must consider very carefully both the existing domestic privacy legislation (including the upcoming Law 81 of 2019) together with applicable international regulations on data protection amid the pandemic, particularly when (i) adopting health control measures in the company's premises (e.g., conducting body temperature checks) to stop the spread of COVID-19 and (ii) implementing new security protocols to protect confidential information of clients and employees when their employees are working from home.
Peru	Existing privacy and cybersecurity-related regulations remain applicable regardless of the COVID-19 crisis and therefore, companies should continue to comply with the existing legal framework. Additionally authorities have stressed the fact that companies should ensure that they have adequate technical and technological capabilities to prevent potential data breaches given the rise in the use of electronic means during these trying times. As a couple of examples, the Banking and Insurance Authorities have issued some guidelines on the continuity of online banking services, stating that banks must ensure that they meet adequate measures against cyberattacks; also, certain regulations regarding remote work state that employers must implement adequate cybersecurity measures while their employees work from home. The following client alert summarizes the main civil, administrative and criminal considerations that companies that operate, collect or otherwise process personal data in Peru, also applicable to companies that are not incorporated in the Peruvian territory but collect data in Peru, should keep in mind: http://rebaza-alcazar.com/blog/alerta-data-privacy-personal-data-protection-cybersecurity-ocassion-covid-19/.
Spain	The health crisis has highlighted the importance of having a good technological structure that can guarantee business continuity in adverse situations. From now on, companies must understand technology as a business ally and must increase the investment made in it. Directly related to the use of technology is the management of network security. This aspect is crucial and all companies should put the focus on it since in these months an increase in security breaches has been detected and it has been demonstrated in many cases that networks are very vulnerable and are not yet prepared for a constant remote working situation.
United States	The transition to remote work environments has created significant new cybersecurity risks, and companies need to be acutely aware of the numerous new vectors for attack (e.g. unsecured home devices and networks, and the use of personal cloud storage accounts to save confidential information) and take steps to mitigate those risks. This is compounded by attackers preying on fears surrounding the crisis to launch social engineering attacks around the COVID-19 pandemic. Companies need to ensure open lines of communication with dispersed employees to provide them with access to and reminders of best practices for securely working from home, as well as the company's remote access and appropriate use policies. Companies should also keep employees updated on emerging risks, as well as proper procedures for elevating potential incidents back to the right personnel and ensuring necessary personnel can respond in a timely manner. Ongoing efforts to stem the spread of the pandemic also mean that many companies will be collecting significantly more data from employees and customers alike, particularly with respect to the health and well-being of any individuals who visit a company facility. While Congress considers legislation specific to the issues raised by data collected and used in the context of the pandemic, companies will need to understand the privacy implications under existing law of measures they may take to promote the health and safety of employees and consumers. Companies should consider exactly what information they need – including, potentially, developing a list of written questions that they deem acceptable to ask – and how their internal and external privacy policies align with any changes in the type, usage, and/or disclosure of information collected, and then make any changes necessary based on new data collection efforts and communicate those changes appropriately.

Uruguay	In the context of the COVID-19 pandemic, companies conducting data processing activities in Uruguay should maintain their compliance and security standards at their highest level. Given the new situation, in which working remotely is becoming the new normal, and new health preventive measures may be required at companies' premises, companies must implement adequate security measures to reduce the risk of data security breaches and respect their employees' privacy rights. Also, when processing and transferring personnel, companies must especially comply with the principles of veracity and accuracy, limited use, data security and proactive responsibility, set forth, respectively, in articles 7, 8, 10 and 12 of the Data Protection Law No. 18.331.
Venezuela	Companies operating in Venezuela should be aware that, although there is no general data protection legislation and no authority is specifically responsible for supervising data protection issues, there are several regulations in place that (a) aim to protect personal data of Venezuelan citizens, (b) regulate the treatment of health data (especially concerning epidemics), and (c) require companies to collect certain data relating to employees' health in a specific manner. There was also a binding decision issued by the Constitutional Chamber of the Supreme Court (Decision No. 1318 dated August 4, 2011) which sets forth several principles regarding personal data collection, treatment and protection, which must be considered in light of the pandemic. Companies should also consider maintaining or strengthening controls over personal data (especially in relation to health data) to guarantee its confidentiality. Finally, companies should take into account the provisions of the Law on Data Messages and Electronic Signatures to properly assess the use of digital media communications with employees working from home, clients and/or suppliers.

2. Has the relevant regulator(s) in your country issued any guidance, rulings, or other public statements about how companies should address privacy or cybersecurity issues raised by the COVID-19 pandemic?

Country	Answer
Argentina	The Argentine Specialized Cybercrime Prosecutor's Unit recently published a series of recommendations to operate safely on the internet, social networks and with online messaging services, in order to avoid personal data theft and online fraud. Moreover, the Argentine Agency of Access to Public Information (Argentina's data protection authority) has shared some recommendations for video calls, such as paying attention to "free" platforms that may use the users' personal data for purposes other than the provision of the service. Lastly, the aforementioned Agency has published a series of recommendations for the use of geolocation apps (whether they are used by the public or private sector, or both in collaboration), and listed fundamental principles on data protection related to them. Useful links (in Spanish): • www.fiscales.gob.ar/ciberdelincuencia/coronavirus-recomendaciones-de-la-ufeci-para-evitar-el-robo-de-datos-personales-cuentas-y-claves-bancarias-durante-el-aislamiento/ (Recommendation of the Specialized Cybercrime Prosecutor's Unit). • www.argentina.gob.ar/noticias/videollamadas-mas-seguras (Recommendation of the Agency of Access to Public Information related to video calls). • https://www.argentina.gob.ar/noticias/proteccion-de-datos-personales-y-geolocalizacion (Recommendation of the Agency of Access to Public Information related to geolocation apps).
Brazil	In 2019, the LGPD was amended by Law No. 13,853/2019 in order to create the Brazilian Data Protection Authority (*Agência Nacional de Proteção de Dados* – "ANPD"). This authoritative body is intended to enforce the new Law and issue regulations and guidelines. Unfortunately, the ANPD has not been created, as the President of Brazil has not yet nominated its members. The creation of the ANPD is crucial, even before the LGPD came into force, because it would regulate the various legal loopholes and provide guidance to Brazilian companies and government bodies on how to comply with LGPD. In addition, the creation of the ANPD would have been crucial since it would have provided greater certainty to companies and governmental bodies on how to comply with the public and private measures issued by the Brazilian government to deal with the COVID-19 crisis. Although these measures are being taken to protect health and prevent crowding, they could have an adverse impact on privacy and data protection.
Chile	As Chile does not have a specific cybersecurity/data privacy agency (it will probably have one once the Data Privacy bill, currently under discussion in Congress, is enacted), all the guidance on this matter has come from each industry-specific regulator. For example, the Undersecretary of Telecommunications has made several cybersecurity recommendations related to the safe use of telecom devices and networks during the pandemic, also launching a public consultation on a proposed draft of a cybersecurity regulation regarding networks and systems used in the provision of telecommunications services. Additionally, the Labor Ministry has issued recommendations on how to implement telework in a manner that complies with local regulations, and the Commission for the Financial Markets has issued several guidelines related to new ways to conduct remote shareholders/board meetings.
Colombia	The following guidance has been issued to date by SIC on how companies should address personal data issues raised by the COVID-19 pandemic:

	• External Directive (*Circular Externa*) No. 001 informs that mobile phone operators and private entities in general have legal grounds to provide to public entities that so require it personal data that is necessary to address, prevent, treat and/or control the spread of COVID-19 and mitigate its effects. The SIC explained that consent to process personal data is not required in the case of medical or sanitary urgency, and when public entities require them to perform their duties. The SIC stressed that public entities must adopt measures to ensure security, restricted circulation and confidentiality of personal data in the context of the emergency raised by the COVID-19 pandemic. • External Directive (*Circular Externa*) No. 002 orders data controllers and processors to refrain from collecting or processing biometric data using physical or electronic fingerprint readers or any other mechanism that allows the spread of COVID-19 through indirect contact, while the emergency endures. This instruction does not apply to biometric identification systems where the device is for personal and individual use. • External Directive (*Circular Externa*) No. 003 extends the deadline for entities to update the registration of their databases before the SIC until July 3, 2020, to control the spread of COVID-19 and mitigate its effects (because information may be at the workplace). The SIC released a public statement through its website announcing that it was requiring certain municipal and provincial authorities to provide information regarding the data processing practices and operations around the mobile app they had launch as a measure to track and control the spread of COVID-19, available at https://www.sic.gov.co/slider/la-superintendencia-de-industria-y-comercio-en-su-calidad-de-autoridad-nacional-de-protecci%C3%B3n-de-datos-se-permite-informar-lo-siguiente-0.
Costa Rica	No, the regulator has not issued any guidance, rulings, or other public statements about how companies should address privacy or cybersecurity issues raised by the COVID-19 pandemic.
Ecuador	Ecuador does not have a regulator for privacy or personal data matters. However, on March 16, 2020, a presidential decree authorized, while the state of exception remains in place, the use of personal data by private companies in coordination with the government to stop the spread of COVID-19. The measures approved allow, without further consent from the data subjects involved, the main Ecuadorian telecommunication service providers to track, through both government and private mobile applications, the location of those persons who must remain confined (e.g., because they have been infected by COVID-19 or they have been exposed to contact with people infected by COVID-19). Furthermore, the Ecuadorian medical law obligates all companies operating in Ecuador to report any possible or confirmed case of COVID-19 among their employees to the government.
Mexico	Yes. The National Institute for Transparency, Information Access and Personal Data Protection ("INAI") has issued several communications that are accessible at the following site: https://micrositios.inai.org.mx/covid-19/
Panama	No guidance or rulings on how to address privacy or cybersecurity issues raised by the COVID-19 pandemic have been issued for companies. However, on April 23, 2020, the Personal Data Protection Council of Panama, composed of nine entities from the public and private sectors, met to analyze the collection, processing and transfer of personal data on the different platforms that are being used to address the state of national emergency decreed by the government because of the COVID-19 situation. The Council particularly emphasized the importance of making correct use of the data collected and the need to raise public awareness of this issue.
Peru	Even though Peru's existing framework has been robust enough to face the current context, Data Protection Authorities have issued an Opinion - "Opinión Consultiva No. 32-2020-JUS" on the processing of health data during the pandemic in the workplace, concluding that: (i) employers may process employees' personal data without their consent when the collection of such personal data is necessary to guarantee safety and health at work in order to prevent the spread of COVID-19, but employers must comply with their obligation to inform employees of these legal provisions; (ii) employees are obliged to cooperate and provide information to their

	employer regarding their possible or actual contagion with COVID-19; and (iii) the processing of personal data carried out by employers in order to prevent the spread of COVID-19 must comply with the provisions of the current Peruvian data protection legal framework.
Spain	Yes, the Spanish Data Protection Agency ("AEPD") has been very active during this health crisis. It has published several notes and different guides about the measures that employers can take to try to control the spread of the virus. Mainly, the AEPD has focused on establishing precisely what the legitimacy is for the processing of health data, and the guarantees that must be applied so that the processing is legal. They have also published a guide to the different technologies used during the pandemic.
United States	Guidance of one form or another has been issued by: the Federal Trade Commission ("FTC"), Department of Homeland Security ("DHS"), Department of Health and Human Services ("HHS"), Department of Education, and the National Institute of Standards and Technology ("NIST"), as well as some states. For example, the Equal Employment Opportunity Commission published guidance concerning the information employers are allowed to collect from employees, as well as the protections that information is due under the Americans with Disabilities Act. HHS issued guidance to entities covered under the Health Insurance Portability and Accountability Act ("HIPAA") on how to appropriately share patients' personal information. Both the FTC and DHS have issued warnings to consumers about scams related to COVID-19 and the risk of clicking on unknown links from unknown senders, and NIST has drafted guidance on security steps companies can implement to reduce the risks posed by employees working from home. Finally, both the FTC and the Department of Education have published guidance on children's and students' privacy in a virtual learning environment subject to protections under the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act.
Uruguay	Yes. The Uruguayan Data Protection Authority ("URCDP") has recently issued Decision No. 2/2020, in which it analyzes and provides guidelines on how Data Protection Law No. 18.331 regulates the treatment of health-related data and sets forth the circumstances under which companies can process health-related data in the context of the COVID-19 pandemic without the data subject's consent. In accordance with this decision, health-related data can only be processed by companies without the data subject's consent under the exceptions set forth in Law No. 18.331, including, among others, when health data is being collected by the government acting within its constitutional powers, when a law establishes that the data can be collected and processed for public interest reasons, when public health is at risk or for epidemiological studies, provided that the data is anonymized. Please see: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/dictamen-2020 Further, URCDP has also issued certain recommendations related to the handling of health-related data. These recommendations include, among others, that companies must (i) implement proactive protective measures, such as data protection impact assessments; and (ii) obtain the subject's written consent to process their personal sensitive data (unless an exception is applicable); this consent may be obtained by electronic means, but, in such cases, measures that ensure the data subject's proper identification must be implemented. Please see: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/recomendaciones-para-tratamiento-datos-personales-ante-situacion Finally, in February 2020, the government issued Decree No. 64/020 which regulates several highly relevant data privacy issues (e.g., the duties of the data protection officer, data protection impact assessments, data breach notification requirements, etc.). We believe that URCDP will continue focusing on issuing guidelines and decisions regarding this type of issue.
Venezuela	No. However, the "state of alarm" decree issued in response to the COVID-19 pandemic requires anyone who is suspected to have contracted COVID-19 or has been exposed to a person with or suspected to have COVID-19 to inform the competent authorities of any useful data to determine the form and extension of possible contagion, emphasizing that the information provided cannot be disclosed or used for any purposes other than those established in the decree (i.e., to stop the spread of the pandemic). In addition, the Ministry of Health reaffirmed the obligation of Venezuelan companies to maintain a registry of employees' chronic illnesses, and included privacy, anonymity, and confidentiality as core principles in the guidelines provided for conducting research related to COVID-19.

3. Are there any changes to existing law that have been undertaken as a result of, indirectly or directly, the COVID-19 pandemic?

Country	Answer
Argentina	Even though there were no legislative changes related to privacy or cybersecurity due to the COVID-19 pandemic, it is worth noting that the health emergency gave rise to complementary regulations impacting privacy. For example, Administrative Decision No. 432/2020 (in force since March 24, 2020) established the mandatory use of the app "COVID-19 Ministry of Health" for anybody entering the country after March 10, 2020 (and permitted the voluntary use of the app for anybody else). Under this context, the Argentine Undersecretariat of Open Government and Digital Country (which depends on the Secretariat of Public Innovation of the President's Chief of Staff Office, and is responsible for the app "COVID-19 Ministry of Health") may process or transfer the personal data collected by such an app (whenever possible, in a dissociated form) to other state entities and/or national, provincial or municipal health facilities, without the need of prior consent of the data subject, to the extent that they do so within their powers pursuant to Article 11 of the Argentine Data Protection Law No. 25,326. Useful link: • https://www.boletinoficial.gob.ar/detalleAviso/primera/227116/20200324 (Administrative Decision No. 432/2020, in force since March 24, 2020, which established the use of app "COVID-19 Ministry of Health").
Brazil	Federal Law No. 13,979/2020 was approved in February in order to impose emergency public health measures in response to COVID-19, and it impacts Brazilian citizens' privacy. Under Article 6, government bodies at the federal, state and municipal levels, and the Federal District must share essential personal data to identify suspected or confirmed COVID-19 cases. The provision makes clear that the sharing of this personal information has the exclusive purpose of preventing the spread of the virus. Likewise, private companies must also share personal data on suspected or confirmed COVID-19 cases with health authorities upon request. This Law also states that the Ministry of Health must maintain public and up-to-date data on confirmed, suspected and investigated cases of COVID-19; while also safeguarding the right to confidentiality of personal information. On April 17th, the President issued Provisional Measure No. 954 (*Medida Provisória* No. 954/2020 or "MP 954")[3], which provides for sharing telecommunications users' personal data with the Brazilian Institute of Geography and Statistics – (*Instituto Brasileiro de Geografia e Estatística* – "IBGE"), for purposes of enabling official statistical research during COVID-19. Under MP 954, telecommunications operators must share with the IBGE a list of names, telephone numbers, and addresses of their customers (individuals or legal entities). MP 954 was justified under the assumption that sharing personal data would allow IBGE to produce official statistics during the pandemic through telephone interviews during the isolation and social distancing measures period. However, the Brazilian Bar Association and several political parties filed lawsuits with the Supreme Court to challenge the validity of MP 954 on the grounds that it would be unconstitutional.[4] They alleged that by requiring telecom operators to make customers' personal data available to IBGE, MP 954 violates the right to privacy, intimacy and data confidentiality as provided by the Federal

[3] Under the Brazilian legislative process, a Provisional Measure (*Medida Provisória* or simply "MP") is an urgent and temporary law issued by the President. It has the same effects as any law approved by the Brazilian Congress (House + Senate) and is valid for 60 days, which can be extended for an additional 60 days, totaling 120 days. For an MP to become a permanent federal law, it has to be approved by the Brazilian Congress within this period. If not approved, the MP is invalidated.

[4] Five direct unconstitutional lawsuits (*Ação Direta de Inconstitucionalidade* – ADI) were filed by the Federal Council of the Brazilian Bar Association - OAB (ADI 6387), the Brazilian Social Democracy Party - PSDB (ADI 6388), the Brazilian Socialist Party - PSB (ADI 6389), the Socialism and Freedom Party - PSOL (ADI 6390) and the Communist Party of Brazil (ADI 6393).

	Constitution. In a landmark decision, the Supreme Court upheld the injunction initially granted by Justice Rosa Weber on the grounds that sharing personal data under MP 954 indeed violates the constitutional right to privacy, private life and data confidentiality. **Recent changes regarding the LGPD's effectiveness** On April 29, 2020, the Brazilian president issued Provisional Measure No. 959 ("MP 959"), which, among other provisions, postpones the effectiveness of the LGPD from August 16, 2020 to May 3, 2021. The publication of MP 959 was totally unexpected, as it occurred during the evaluation of the Senate's Bill No. 1179/2020 by the Brazilian House of Representatives, which, among other matters, proposes delaying the LGPD's effectiveness to January 1, 2021, whereas its administrative sanctions applicability (including fines) would only be applicable as of August 1, 2021. Finally, Bill No. 1179/2020 was signed by the President on May 10, 2020 and published in the Official Gazette as Law No. 14,010/2020. Considering that MP 959 must be approved by the Brazilian Congress in order to become a permanent federal law, it is not clear at this point when the LGPD will effectively come into force, and that is causing confusion and legal uncertainty for companies, especially foreign investors. Therefore, the current scenario for the LGPD's effectiveness is as follows: • **Entry into force**: May 3, 2021, under MP 959/20's terms. • **Enforceability of administrative sanctions**: August 1, under the recently enacted Law No. 14,010/20. However, if 959/20 is not approved by the Brazilian Congress, the LGPD will come into force in August of this year, as described below: • **Entry into force**: August 16, 2020, under Law No. 13,853/2019, which amended the original LGPD text. • **Enforceability of administrative sanctions**: August 1, 2021 under the recently enacted Law No. 14,010/2020. In any event, the fact that the administrative sanctions of the LGPD will come into effect only in August 2021 does not preclude the enforcement of administrative sanctions foreseen in other laws dealing with privacy and data protection matters, such as the Consumer Protection Code and the Brazilian Internet Law (*Marco Civil da Internet* – "MCI"). These administrative sanctions could be enforced by other public authorities, such as the Public Prosecutor's Offices and consumer protection agencies. Moreover, the postponement of enforceability of the LGPD's administrative sanctions does not preclude other means of enforcing the LGPD provisions after this Law comes into effect, as data subjects, the Public Prosecutor's Offices and private associations, for example, will still be able to file law suits in courts to enforce the provisions of the LGPD and seek redress. Not knowing when the LGPD is effectively coming into force and not having the respective authority – the ANPD – to oversee the LGPD are two aggravating problems amid the COVID-19 crisis. Therefore, it is crucial that the Brazilian Congress approves MP 959/20 as soon as possible to put an end to the uncertainty surrounding the date on which LGPD will enter into force.
Chile	We have not seen concrete changes or modifications to laws, but a group of Senators have proposed a draft bill that modifies the current legislation in order to allow city councils (municipalities) to collect and process sensitive data such as health conditions of the residents in their territories. Another legislative initiative recently submitted to the Congress proposes to mirror in Chile some of the rights, principles, obligations and other provisions from the European General Data Protection Regulation in order to improve Chile's data protection and privacy regulations. The above-mentioned initiatives are currently under discussion and will probably follow a very straightforward path to be enacted as laws of the Republic.

LATAM COVID-19 Task Force – Privacy and Cybersecurity Issues

Colombia	No.
Costa Rica	There have been a significant number of changes to existing laws because of the COVID-19 pandemic. However, none of these changes has addressed privacy or cybersecurity matters.
Ecuador	As mentioned above, though privacy rights are recognized and guaranteed by the Ecuadorian Constitution as fundamental rights, there are no specific privacy regulations and regulatory authorities. However, as a consequence of the COVID-19 pandemic, the national assembly has resumed the analysis of an old draft privacy law that was previously postponed for months. PBP is part of the group of experts advising the senators on the drafting of the law. For further information, please refer to the links below: • https://www.pbplaw.com/es/que-tan-protegidos-estan-mis-datos-personales/ • https://www.pbplaw.com/es/webinar-pbp-proteccion-de-datos-personales-de-sus-empleados/ • https://www.pbplaw.com/es/que-significa-la-proteccion-de-datos-personales/
Mexico	No.
Panama	There have been a number of laws and regulations passed as a result of the COVID-19 pandemic to address health, labor and fiscal issues. However, none of them are related to data protection, privacy or cybersecurity matters.
Peru	The Opinion issued by the Data Protection Authorities is considered confirmation of the Data Protection Authorities' criteria in applying the actual legal framework, not a change to existing laws. Additionally, a practical guide has been published in order to orient healthcare establishments processing sensitive data related to COVID-19 patients. You may find a brief summary of the matter in the following client alert: http://rebaza-alcazar.com/blog/alerta-data-privacy-guide-healthcare-establishments-regarding-covid-19/
Spain	With regard to data protection regulations, no. The regulations themselves include exceptional situations for public health reasons that enable data to be processed. Only a ministerial order has been published which covers the type of applications that can be developed to prevent the spread of COVID-19, but it does not modify the current regulations in any way.
United States	No. Several members of Congress have introduced legislation explicitly focused on protecting consumer information collected for COVID-19-related purposes, but it seems unlikely that any such privacy legislation will be enacted in the short term. At the state level, the California Attorney General has declined to delay the enforcement date for the California Consumer Privacy Act (currently set for July 1).
Uruguay	No. Existing laws and regulations in Uruguay have not been modified as a result of the COVID-19 pandemic.
Venezuela	There are no other changes to existing data protection or cybersecurity regulations than those described above.

4. What are some of the key/repeat questions you have heard from clients trying to deal with the privacy and cybersecurity issues raised by COVID-19?

Country	Answer
Argentina	Most clients have inquiries on (i) how to handle personal data of their employees who may have tested positive with COVID-19 and (ii) how and if they can or should check employees' temperatures before they are granted access to the company's premises, as well as doubts or concerns about employees' expectation of privacy when performing their work-related tasks. In addition, we have received frequent questions on how to ensure general privacy policies and cybersecurity measures remain in force and effect.
Brazil	Most of the questions are related to how companies may process employees' sensitive personal data, whether companies may carry out testing, what precautions must be taken, and how to handle sensitive personal data related to COVID-19 after the end of the pandemic. There are also questions about privacy and cybersecurity concerns related to telecommuting, including how to implement an incident response plan adapted to this new situation.
Chile	Most of the questions that we have received from our clients are related to the possibility of creating databases and records with personal information of their employees, specifically information on underlying chronic medical conditions. This matter is strictly regulated under Chilean legislation, as these types of databases implicate the treatment of sensitive personal data and must comply with strict conditions in order to be legally collected and used.
Colombia	Companies are asking constantly about the best way to balance their obligations under Colombian data protection laws, and their duties to implement health protocols to prevent the spread of COVID-19 when they resume activities. This has been particularly challenging for them given the absence of specific and comprehensive guidance on the part of SIC. Companies are also asking about their cybersecurity obligations under local law, considering the need of businesses to have their employees work from home in less secure environments.
Costa Rica	The most frequent questions that we have received from our clients are related to how to manage (collect and use) sensitive personal information and how companies should treat an employee suspected of having COVID-19. We are also receiving questions in connection with the "working from home" regulations recently enacted.
Ecuador	Most of our clients, which are large domestic companies and multinationals, are concerned about whether their data privacy protocols are in compliance with the applicable regulations and, particularly, with the above-mentioned COVID-19 specific report obligations. Therefore, they are constantly requesting our advice to assess and confirm that they are complying with the obligation to report confirmed and possible COVID-19 cases and that, at the same time, the safety and preventive measures that they are implementing to comply with such obligation do not constitute a violation of the privacy or personal data protection regulations.
Mexico	Frequent questions are: What personal data can be collected related to COVID-19 patients? Answer: All data deemed relevant to Mexican health authorities, in view of the emergency situation, that could potentially harm a person or when the personal data is necessary for the treatment, prevention, diagnosis and provision of healthcare. Is it necessary to obtain the consent of the holder of personal data related to COVID-19? An exception to obtaining the express written consent of the holders could be considered while processing data related to the emergency, provided that said data is necessary for medical care, prevention, diagnosis, the provision of healthcare, medical treatments or the management of health services. Such exception would apply as long as the holder is not in a position to grant consent or when there is

	an emergency situation that could potentially harm such person. It will therefore be essential that the controller analyzes case by case in order to determine which one may be subject to the exception, and in case of uncertainty, the applicability of the exception should be confirmed by INAI or the applicable local authority. Is it necessary to include COVID-19 in the controller's Privacy Notice? Yes. The processing of personal data derived for the COVID-19 crisis must be informed, and the owner of such personal data must know at all times the purposes for which his or her personal data will be collected and processed. Prior to the processing, the controller must make its privacy notice available to the owner. Is it necessary to establish security measures in any organization or authority for the processing of personal data obtained due to the COVID-19 crisis? Yes. Controllers must comply with their obligations of security and confidentiality and therefore must take the necessary physical, administrative and technical measures to guarantee the integrity, availability and confidentiality of the information, given its sensitive nature. What kind of security measures should any organization or institution take in order to address the ongoing remote work? If staff work remotely and through personal devices, the same security measures taken to protect the organization's information under normal circumstances should be taken, or even adopt new ones if required, as remote work increases the risk of loss or leakage of information that may contain personal data. It is also suggested to communicate through channels established by institutions and to avoid the use of internet pages or unverified mobile applications for the flow of information. Can I request additional health information from employees due to COVID-19? We recommend that employers encourage workers to voluntarily report symptoms or relevant COVID-19 information rather than have employees fill out extensive forms about their health situation or frequent destinations, as they may be disproportionate. Is it necessary to document the decision-making process derived from COVID-19? Yes. It is necessary to document the decision-making process related to the processing of sensitive personal data in order to comply with the principle of responsibility, as well as to take steps to notify staff about how their personal information will be handled to respond to any potential or confirmed case of COVID-19. Can staff be informed that a co-worker or visitor to the institution or organization contracted or can be a suspected case of COVID-19? As part of the obligation to safeguard the health and safety of workers, staff can be informed that a co-worker or visitor contracted or may be a suspected case of COVID-19. However, this information will be provided anonymized in order not to make the affected person identifiable, and thus avoid a situation of tension and even discrimination. Can I share employee health information with public health authorities? Yes, but only if required by a health authority when updating an exception scenario for the transfer of personal data. However, such communication must observe compliance with the other guiding principles and duties of the right to the protection of personal data.
Panama	So far, we have not received any questions related to privacy or cybersecurity issues raised by COVID-19.
Peru	Clients have been mostly concerned about whether or not the collection of their employees' personal data (e.g. weight, body measurements and other health-related data), for the purpose of the identification of risk factors and the development of protocols for resuming activities, imposes additional obligations that should be taken into account. As previously mentioned, any such sensitive personal data collected by companies shall be treated in accordance with the existing applicable regulations.

LATAM COVID-19 Task Force – Privacy and Cybersecurity Issues

Spain	The most recurrent queries we have received have been in relation to the processing of health data by employers with respect to their employees and customers. These consultations have focused on two different procedures: • the possibility of requesting health information from workers and customers or even of accessing the results of COVID-19 tests; • the possibility of incorporating thermal cameras to measure the temperature of workers and customers.
United States	Questions related to best practices for collecting, using, securing, and sharing employee data related to COVID-19 – e.g., what questions can we ask, how long should we save it, what can we do with the information, etc. – continue to be at the forefront of companies' minds, particularly as many states have withdrawn their stay-at-home orders and companies begin to welcome their employees back to the office.
Uruguay	The key questions we are receiving from clients are the following: • How to process health-related employee data in the context of the COVID-19 pandemic? • How to validly obtain consent from data subjects in order to process health-related data? • How to implement remote working in compliance with applicable data protection regulations?
Venezuela	Clients have recently asked about the appropriate manner to collect and process personal data related to the issues raised by the pandemic (e.g., health data), and about the requirements for conducting legitimate international data transfers amid the pandemic.

5. What do you anticipate the medium- and long-term effects of COVID-19 will be on privacy/cybersecurity issues? For example, do you think this will make it more/less likely that new legislation will be enacted related to privacy? Will it change how much and what kinds of information companies collect about their employees?

Country	Answer
Argentina	Surely, COVID-19's effects regarding privacy and cybersecurity will persist even after the health emergency ends, or the mobility restrictions related to the health emergency become more flexible. For example, Provision No. 4/2020 (in force since May 21, 2020), which approved and made public the terms and conditions of the "COVID-19 Ministry of Health" app, states that the data related to geolocation will be preserved only as long as necessary (i.e., as long as the health emergency lasts), although anonymized versions may be preserved for scientific and epidemiological purposes. On the other hand, the effects of COVID-19 could make it more likely for new legislation to be passed. In this regard, in September 2018 the Argentine Executive Branch introduced before Congress a bill intended to replace the Argentine Data Protection Law, arguing that it has become outdated given recent technological and legal developments, especially regarding the recent implementation of the GDPR in the EU. This draft bill lost parliamentary status in March 2020, so it is likely that a new proposed text, following a similar GDPR style, could be introduced during 2020 (in fact, the Argentine Data Protection Authority mentioned this as part of its 2020 plans).
Brazil	As to the medium- and long-term effects of COVID-19, we envision that companies will be more and more engaged with digital transformation, which will require more caution with privacy and cybersecurity measures to protect corporate confidential information and personal data. Companies will have to review and improve their systems and internal policies to ensure the security of telecommuting. We also envision an increase in testing and other health monitoring efforts by companies and public entities, which may result in large-scale processing of sensitive personal data. The increasing reliance on massive testing and monitoring will raise concerns on privacy and data protection matters, and this will likely result in legal disputes and/or legislative initiatives. Several state governors and local city governments have entered into partnership arrangements with telecommunications and technology companies to enable collecting aggregated and anonymized geolocation data in order to monitor crowding and social distancing rates. The reliance on technology aiming to control the effects of the pandemic is expected to remain until the end of the COVID-19 crisis. It is also expected that there will be an increased use of tracing apps by governments and companies to keep tracking individual smartphone users' real-life interactions with other smartphone users in order to control and/or prevent contacts with individuals suspected or confirmed of having COVID-19. This may also result in a legal debate within the upcoming months.
Chile	As previously mentioned, one of the most substantial changes that our privacy and cybersecurity legislation has ever faced (the creation of a specific cybersecurity/data privacy regulator) is being pushed forward amid the pandemic. The protection of individuals' personal and sensitive data and the confidentiality of strategic information have become a key aspect in a society that now bases its relations in remote communications. The new legislation that will most likely be enacted in Chile will include the creation of a specialized privacy agency that will be able to impose severe sanctions to companies not complying with the new standards, while also empowering data subjects with rights that are not currently covered by legislation.

	More information about Chile recommendations are available at https://www.bye.cl/covid-19-recomendaciones-relativas-a-teletrabajo-seguridad-de-la-informacion-y-proteccion-de-datos-personales/
Colombia	Given the absence of guidance from SIC regarding the obligation of businesses to implement health protocols to prevent the spread of COVID-19 when they resume activities (which requires them to collect and process personal data), we anticipate widespread enforcement activity looking into data processing operations conducted by businesses in this regard. We do not anticipate new legislation being enacted related to privacy due to the COVID-19 pandemic, but we consider it is likely that cybersecurity will be at the top of the legislature's agenda in the near future – Colombia does not have comprehensive legislation regarding cybersecurity obligations, but rather sectoral (i.e., for financial institutions).
Costa Rica	We foresee that the COVID-19 pandemic will change the existing regulation on sensitive personal data. Also, companies may allocate in the future more resources to address cybersecurity protection issues and to train their employees to teach them how to avoid conduct that may have a negative impact on the technology and information systems and data protection policies of the company. For further information, please refer to the following link: https://www.blplegal.com/es/Biblioteca-COVID19-Coronavirus-Centroamerica
Ecuador	For Ecuador, COVID-19 has been a breaking point. The president recently declared that all regulations related to digital matters, including privacy and cybersecurity, are now a priority. The country is going through a digitalization process and new specific laws for matters such as privacy are necessary. Indeed, as mentioned above, as a result of the pandemic the national assembly has resumed the analysis of the draft of the first Ecuadorian privacy law that was previously postponed for months. We believe that the pandemic will affect the behavior of the companies on how they collect data. For example, although we currently know very little about COVID-19, getting and processing information related to COVID-19 in future hiring processes could help companies to be prepared for the so feared "second wave" or other future similar health crises.
Mexico	It is foreseeable that administrative data protection regulations will be reinforced by criminal provisions mandating corporations to implement compliance programs.
Panama	We anticipate new biosecurity measures to be implemented as lockdowns wind down and more companies resume their activity, which, may raise privacy issues. In our opinion, more guidance and rules related to privacy will be forthcoming in the near future. In this regard, it is a fact that social and business relations and governmental processes have already changed due to COVID-19. As a result, it is imperative to adapt the existing regulations to further protect personal data and the individual's right to privacy.
Peru	From a regulatory point of view, we expect applicable regulations to remain unchanged in the short- and medium-term. However, we do expect the issuance of more opinions by the Data Privacy Authority to help companies navigate through the COVID-19 crisis.
Spain	There is currently an emerging debate about what should prevail, whether public health or the right to privacy and data protection. Despite the fact that on the part of society there is a more permissive view of data protection, the AEPD has expressed the importance of this and has clearly established that, although situations of health crisis exist, data protection must continue to be respected. The main challenge that companies are now going to face is a technological challenge, since the way of working has been modified and it has been demonstrated that many companies have not been able to face this new way of working because they do not have good technological structures. Likewise, the main risks will be linked to cybersecurity, and to the implementation of adequate security measures for each system to prevent the violation of systems and access to restricted information.
United States	The COVID-19 pandemic has forced companies to stress test their networks and contingency policies and plans in an unprecedented way. The unintended benefit may be that companies will use this as an opportunity to ensure that their cybersecurity and network assets are more agile, responsive, and robust than before the crisis. It does not appear the pandemic will have much effect on legislation in the privacy or cybersecurity spheres. While the crisis has highlighted many of the issues that companies must face in complying with multiple, confusing, and often overlapping state and

	federal laws, it has not helped to resolve some of the fundamental issues that continue to impede efforts at comprehensive federal privacy legislation.
Uruguay	We do not expect new legislation to be enacted in the short term as a consequence of the COVID-19 pandemic; we believe that URCDP will continue to actively issue decisions and guidelines regarding specific privacy-cybersecurity issues. Regarding the medium and long term effects, new legislation could be enacted, particularly to address the treatment of health-related data in more detail than current regulations. However, we do not expect a significant change on the quantity and type of employees' personal information that companies will be allowed to collect or treat. Uruguayan current regulations include clear principles and boundaries on the collection and treatment of personal data, which inherently limit the amount and type of employees' personal data that companies can collect. As a consequence, we believe that future regulations would focus on a more detailed analysis of specific issues, rather than on new limitations. Please see our report on Decree No. 64/020: https://www.guyer.com.uy/en/what_we_do/news-knowledge/on-line-news/informe-especial-modificaciones-en-materia-de-proteccion-de-datos-personales/. Please see: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/recomendaciones-para-tratamiento-datos-personales-ante-situacion. Please see: https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/dictamen-2020.
Venezuela	We believe that companies in Venezuela will increase the amount of health information collected to protect the labor environment and will take additional security measures to guarantee the safety of such data, and the use of teleworking tools. This will probably prompt Venezuela to enact new legislation related to privacy or cybersecurity in the short term.

Willkie has multidisciplinary teams working with clients to address coronavirus-related matters, including, for example, contractual analysis, litigation, restructuring, financing, employee benefits, SEC and other corporate-related matters. Please click here to access our publications addressing issues raised by the coronavirus. For advice regarding the coronavirus, please do not hesitate to reach out to your primary Willkie contacts.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Maria-Leticia Ossa Daza
212 728 8146
mossadaza@willkie.com

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Nicholas Chanin
202 303 1164
nchanin@willkie.com