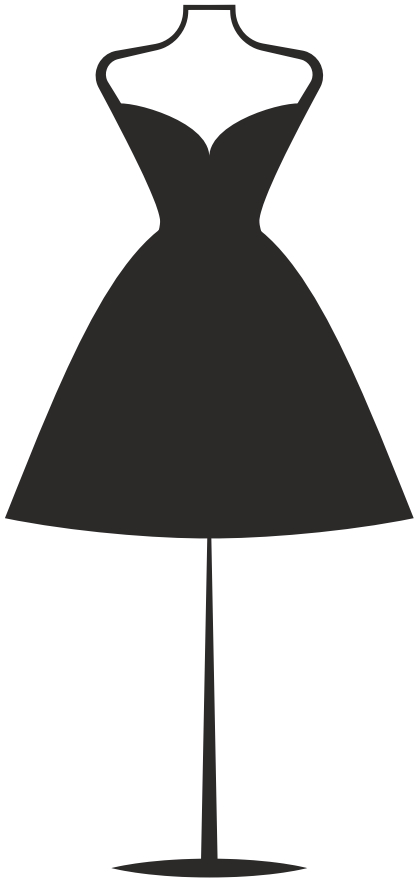

REGULATING CLOUD COMPUTING

BY
MAX LUTZE

Max Lutze is a lawyer and an Associate in the Privacy & Data Protection practice at Grant Thornton LLP.

Visit www.competitionpolicyinternational.com for access to these articles and more!

REGULATING CLOUD COMPUTING

By Max Lutze

More and more businesses are shifting to cloud computing for their data management strategies. Simultaneously, questions surrounding regulatory obligations continue to arise, not because of the complex nature of existing regulations, but because of the lack of any that actually address cloud computing by name. At the same time, privacy law's rapid evolution means that it is only a matter of time before the law catches up to this technology. The legal landscape remains unclear, but businesses would do well to develop compliance programs that satisfy current legislative frameworks and prepare them for the inevitable arrival of laws that do impose obligations upon both the users and providers of cloud services.

In fashion, trends come and go. But every now and then a designer forever transforms the way people dress, and in technology, the cloud is no different. Much like Coco Chanel's Little Black Dress quickly made its way into the meaning of a complete women's wardrobe, in the world of electronic data, storing data in the cloud is becoming the new norm for companies' data management strategies.

The advent of cloud computing enables companies to keep one finger on the data they manage at all times as well as have a seemingly infinite amount of space to store it. However, even if moving to the cloud obviates the need for on-premise storage systems, there is still a strong impetus to responsibly manage that virtually stored data. But whether that obligation is merely moral or also legal is a blurred line.

While data privacy in general has been and continues to be regulated, the law still lags behind when it comes to cloud computing. In the absence of direct regulation, however, there are a few key themes to which companies will want to pay particular attention as they embrace this latest, transcendent piece of technology.

01
CLOUD COMPUTING AND BUSINESS

The business landscape as it relates to cloud computing has changed considerably since the start of the worldwide COVID-19 pandemic. More companies are moving to the cloud, particularly as remote work has become a much more standard practice for many employers.[2] According to a 2022 survey by marketing technology company Foundry, 69 percent of organizations surveyed have accelerated their transition to the cloud since 2021, and Foundry forecasts that at least 63 percent of companies will have nearly all of the IT infrastructure in the cloud by the end of 2023.[3] A driving factor behind this rapid effort to rely on cloud computing is the benefits of cloud computing as compared to on-premise data storage systems. Whereas cloud computing offers more storage at far lower costs, on-premise storage can quickly become expensive, as more data requires more physical space. While cloud-based systems provide strong security protections, notably in the form of encryption, on-premise storage relies heavily on physical and human security resources. Likewise, recovery mechanisms for data lost in the cloud are much stronger than those that exist for physical data.

While the list of why cloud computing is better than on-premise storage as a data management tool is certainly a long one, there are valid concerns associated with using the cloud. First, cloud services are often provided by third parties. This means that, depending on the storage model a company chooses, visibility and control over the data being stored can be considerably reduced.[4] Additionally, while cloud computing does offer enhanced security protocols, cyber attacks are still a very real threat. In 2022, the United States Cybersecurity & Infrastructure Security Agency warned that the Russian invasion of Ukraine could expose more U.S. companies to Russian cyberattacks.[5] Meanwhile, the Cloud Security Alliance, which sets international standards and best practices for cybersecurity, expects that by 2030, a quantum computer will be able to break current cybersecurity infrastructure.[6] Finally, there are jurisdictional challenges for companies using cloud computing to meet. Data may not be stored in the country in which it is collected, and this can and will pose difficulties in meeting relevant regulatory obligations.

02
THE LEGAL LANDSCAPE

Regulating data privacy is at the forefront of legislators' minds across the globe. From the European Union to Singapore to Brazil, privacy laws are being integrated into the legal fabric of countries around the world. That said, while many of the existing laws may touch on cloud computing, there are very few, if any, that actually regulate it. The prevailing approach among those countries that do have laws that address this topic is to institute requirements that are

2 The Upwork Team, Upwork (Sept. 7, 2021), https://www.upwork.com/resources/moving-to-cloud.

3 *Cloud Computing Study 2022*, Foundry (Apr. 6, 2022), https://foundryco.com/tools-for-marketers/research-cloud-computing/.

4 *Id*.

5 *Russia Cyber Threat Overview and Advisories*, Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/uscert/russia.

6 *Cloud Security Alliance Sets Countdown Clock to Quantum*, Cloud Security Alliance (Mar. 9, 2022), https://cloudsecurityalliance.org/press-releases/2022/03/09/cloud-security-alliance-sets-countdown-clock-to-quantum/.

inherently tied to cloud computing but do not necessarily refer specifically to that technology.

China, for example, continues to pass strict data privacy laws that cast a wide net in terms of the regulatory objectives they fulfill. As regards cloud computing, the most recent of these new laws, the 2021 Data Security Law ("DSL") and Personal Information Protection Law ("PIPL"), place a particular emphasis on data localization requirements. Under both laws, covered entities are required to store and process any collected data within China itself.[7] By implementing this obligation, and leveraging the threat of tough financial and criminal penalties for non-compliance,[8] China is seemingly reigning in one of the key features of cloud computing (the ability to store and access data anywhere) without directly referring to it in the text of a law.

Likewise, in Singapore, the Personal Data Protection Act (PDPA), which passed in 2012, does not cover cloud computing. However, the Personal Data Protection Commission ("PDPC"), which is responsible for enforcing PDPA, released a set of advisory guidelines in May of 2022 that address cloud computing.[9] These guidelines focus on the roles and responsibilities both of organizations that use cloud services providers ("CSPs") and of CSPs themselves as regards compliance with PDPA. Under the guidelines, companies that use cloud services are responsible for complying with all of PDPA's standard data processing requirements. This, in essence, does not really introduce a novel understanding of a company's obligations under the law.

Where the guidelines do add to what PDPA is lacking is in the interpretation of the obligations of CSPs. According to the PDPC, CSPs that process personal data on behalf of their customers are considered data intermediaries and subject to the protection and retention limitation obligations under PDPA.[10] While such requirements are, as mentioned earlier, not found in the original text of PDPA, they do at least demonstrate that Singapore's primary data privacy regulatory body is contemplating the evolving landscape and that enforcement actions may in fact apply to CSPs as well as their clients.

Turning to the European Union, there is less regulatory material to rely on. The General Data Protection Regulation ("GDPR"), while a robust exemplar for many new privacy laws around the world, does not directly regulate cloud use or cloud service providers; instead, it imposes a variety of traditional privacy requirements and outlines various rights that must be guaranteed.[11] In effect, the role of GDPR in cloud regulation is to pull cloud computing under its long arm to the extent currently possible by implying that elements essential to any standard privacy program in the EU, such as retention schedules, breach responses, and data ownership and portability considerations, are contemplated equally by companies and CSPs alike.[12]

Regardless of which geographic region one examines, the story is likely to be similar everywhere. Cloud computing is not at the heart of any regulation, but those laws that do exist are trying to ensure that the same obligations that apply to businesses that use on-premise storage or engage in cross-border data transfers apply to those that use cloud services, as well as to those providing those services.

03

CONSIDERATIONS FOR BUSINESSES

With a sense of the regulatory landscape in mind, it is worth discussing three broader areas of electronic data management as they relate to data controllers and processors. Cross-border transfers, data localization requirements, and the overall patchwork nature of cloud regulation are all ele-

7 Todd Liao, *Navigating China's Data Protection Laws*, Morgan Lewis (Mar. 1, 2022), https://www.morganlewis.com/pubs/2022/03/navigating-chinas-data-protection-laws.

8 DigiChina, *Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)*, DigiChina (June 29, 2021), https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/.

9 Personal Data Protection Commission, *Advisory Guidelines on the PDPA for Selected Topics 17 May 2022*, Personal Data Protection Commission (May 7, 2022), https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-the-PDPA-for-Selected-Topics-17-May-2022.pdf.

10 *Id*.

11 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

12 Alex Tolsma, *GDPR and the Impact on Cloud Computing*, Deloitte, https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-update-the-impact-on-cloud-computing.html.

ments that may influence a business's cloud data management strategy.

As for cross-border data transfers, the most high-profile area of complication involves transfers between the European Union and the United States. What businesses must understand with regard to this is that under GDPR, data transfers to a jurisdiction that lacks an equivalent level of protection to the EU regulation are prohibited in the absence of adequate safeguards.[13] Since the European Court of Justice invalidated Privacy Shield, which previously governed EU-US data transfers, in 2020, the certainty with which a business can determine it is legally transferring data collected in Europe to the United States remains eroded. In the meantime, a new data transfer policy, although in development, has not yet been approved.[14]

> ***"As for cross-border data transfers, the most high-profile area of complication involves transfers between the European Union and the United States***

The effect this limbo has is that the very nature of cloud computing has a potential to run afoul of EU law. Businesses must be conscious of the fact that while storing data in the cloud may be purely a data management tactic, the location in which that data is being stored is something the business may be responsible for knowing. Likewise, CSPs, although likely considered to be processors rather than controllers under GDPR,[15] are still required to comply with restrictions on cross-border transfers.[16] Of note, however, is that GDPR Article 40 gives entities the right to develop codes of conduct that contemplate, among other things, policies regarding cross-border transfers.[17] By drafting an Article 40 code of conduct, CSPs can demonstrate that they understand their compliance obligations.

Data localization obligations are equally important for businesses to consider in developing a cloud data management strategy. Localization is, like cross-border transfers, intertwined with cloud computing because of the aforementioned reduced visibility cloud users have when it comes to where data is stored. This article touched earlier on how China's DSL and PIPL handle localization, and in Europe there has been a similar push to keep data within the EU as much as possible.

A new proposal from EU authorities creates several levels of cybersecurity certification, the highest of which would essentially compel businesses that provide certain services to use European CSPs so as to ensure that the EU's data localization objective is being achieved.[18] As localization is an integral part to any comprehensive privacy legislation, businesses should understand that by incorporating a localization strategy into their cloud storage program, they put themselves in a position to be better prepared not only for existing compliance requirements, but for developments in localization policy as well.

A final practical consideration for businesses either currently managing or planning to manage their data in the cloud is that regulation of this field is by no means cohesive. While privacy laws generally may mirror each other regardless of jurisdiction, relying upon them to dictate how cloud computing will be addressed from a legal perspective simply is not realistic at the moment. In fact, it appears unlikely that there will be distinct, standalone laws for cloud technologies. It is more likely that these will be touched on in a variety of regulations that focus on adjacent considerations. In Europe, the EU after GDPR is regulating data-related areas almost by subject.

The Digital Markets Act, Digital Services Act, eCookie Directive, Data Act, and several others are all designed to cover interconnected areas of data privacy. In the United States, new comprehensive state laws, such as CCPA, CPRA, and CDPA, are joining existing sectoral regulations like HIPAA and GLBA. Companies should therefore not necessarily wait until one of these new laws addresses cloud

13 Luca Bertuzzi, *Is Data Localization Coming to Europe?*, International Association of Privacy Professionals (Aug. 23, 2022), https://iapp.org/news/a/is-data-localization-coming-to-europe/.

14 Axel Spies et al., *EU Commission Begins Process to Adopt Adequacy Decision for EU-US Data Privacy Framework*, Morgan Lewis (Dec. 15, 2022), https://www.morganlewis.com/blogs/sourcingatmorganlewis/2022/12/eu-commission-begins-process-to-adopt-adequacy-decision-for-eu-us-data-privacy-framework.

15 Peter Church & Caitlin Potratz Metcalf, *U.S. CLOUD Act and GDPR – Is the Cloud Still Safe?*, Linklaters (Sept. 13, 2019), https://www.linklaters.com/en/insights/blogs/digilinks/2019/september/us-cloud-act-and-gdpr-is-the-cloud-still-safe.

16 *Impact of GDPR on Cloud Service Providers*, Fortra (May 23, 2021), https://www.tripwire.com/state-of-security/impact-of-gdpr-on-cloud-service-providers.

17 *Supra* note 10.

18 Vincent Voci et al., *Issue Briefing: The European Union's Proposed Cybersecurity Certification Scheme for Cloud Services (EUCS)*, U.S. Chamber of Commerce (Dec. 5, 2022), https://www.uschamber.com/security/cybersecurity/issue-briefing-the-european-unions-proposed-cybersecurity-certification-scheme-for-cloud-services-eucs.

computing specifically. Instead, the initiative really lies with them, and this refers both to the effort to preemptively be as compliant as possible and to consider the implications of operating in certain jurisdictions.

Where feasible, it may be wise to avoid doing business in places where the local authorities have strict laws whose aim is perhaps to penalize companies rather than address legitimate privacy concerns. The high monetary fines and extremely short remediation periods in Chinese privacy law make no exceptions, not even for Chinese companies.[19] By taking these factors into account, businesses may find themselves better equipped to handle regulatory obligations as they evolve and inevitably become pertinent.

04
CONCLUSION

Cloud computing is permanently changing the way businesses manage data. There will likely be no future in which organizations do not view it as a necessary part of business operations. As such, it will naturally be subject to regulation in one form or another, even if that form is only one from which businesses can only ever draw inferences or suggestions on how to obey the law.

Companies can prepare by approaching compliance with potential cloud computing regulations with the same attitude they adopt for existing comprehensive privacy laws. They can ensure, for example, that their cloud service provider only transfers data to locations with data protection regimes equivalent to the national one. They can treat the use of a CSP the same way they would treat the use of traditional IT methods for data management, by presuming that cloud computing demands full compliance with any relevant privacy legislation. Finally, they can tailor their business models and data management strategies to the locale by assessing the sensibility of using cloud services in more restrictive countries.

In the absence of a standardized framework, and even despite more defined regulations worldwide, such as GDPR, companies should still go through the process of rationalizing requirements based on their obligations under applicable laws, their business objectives, their strategy, their priorities, and create their own framework for implementing and enhancing an approach that is sustainable and scalable. ■

> ***Cloud computing is permanently changing the way businesses manage data***

19 InCountry Staff, *China's New Personal Information Protection Law Raises the Stakes*, InCountry (Aug. 26, 2021), https://incountry.com/blog/chinas-new-personal-information-protection-law-raises-the-stakes/.

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL