



WHITE PAPER

***Evolving data regulations
pave the way for telcos'
transition to the public cloud***

Hyperscalers allow telcos to specify where their data resides and how they can encrypt their data at motion or at rest in the public cloud.

EXECUTIVE SUMMARY

The public cloud presents a huge opportunity for telecom operators to improve the subscriber experience, reduce churn and gain operational efficiencies. So why has the industry been slow to adopt it? An often-stated concern is that data sovereignty regulations prevent the transfer of sensitive user information to the public cloud.

That's not the case anymore. Data protection authorities around the world are evolving their regulations to allow data transfer within their own borders, as well as to other approved countries. Even if there are currently no public cloud regions in locations that meet your regulation criteria, there are other options that allow telcos to begin to use the public cloud. Plus, hyperscalers continue to build out new regions and offerings. With the length of time it will take telcos to move thousands of workloads to the public cloud, telcos can confidently start to move their IT stack to the public cloud now.

Mobile operators should seize the flexibility, scalability, cost-savings and revenue opportunity offered by the public cloud as soon as possible. If you think data sovereignty requirements are keeping you from using the public cloud, it's time to do a deep dive on what's changed.

Five steps to ensure data regulation compliance

Follow these steps to learn how to comply with applicable data regulations for the countries where you operate:

- 1 Check the regulations** that apply in the countries where you operate. We find the [OneTrust DataGuidance™ tool](#) to be a handy reference. Note that in some countries there are specific rules for telecommunications data.
- 2 Read how the hyperscalers—[AWS](#), [Azure](#), [GCP](#)—address** different privacy and security issues. In particular, make sure to check the certification pages for each one: [AWS](#), [Azure](#) and [GCP](#).
- 3 Understand how you can specify** where your data resides and how you can encrypt your data at motion or at rest here: [AWS](#), [Azure](#) and [GCP](#).
- 4 Check where the [AWS](#), [Azure](#) and [GCP](#) data centers are located** and see if there is one in your country, or in a location where you are able to host your data.
- 5** If you cannot find a suitable hyperscaler data center in which to host your data, another approach is to **see if your local data protection authority allows** you to use preapproved contractual clauses or submit requests for approval to use the public cloud.

INTRODUCTION

Organizations of all sizes, across industries are moving their IT operations to the public cloud. Hyperscalers such as Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) seem to be taking over the information technology (IT) world.

For mobile operators, this technology shift requires new capabilities and provides new opportunities. But the telecoms industry is still reluctant to move their systems to the public cloud. Most telcos host their operations support systems (OSS) and business support systems (BSS) on physical servers in their own data centers.

Telcos should embrace the powerful functionality that the hyperscalers provide to achieve lower capital costs, better disaster recovery, more resiliency, flexibility and scalability. So why aren't they?

According to a TM Forum survey, privacy and security are top concerns for telcos, with more than 70% of respondents ranking them as key barriers preventing public cloud adoption.

70%
of telcos rank
privacy and
security as
top concerns
hindering public
cloud adoption

Communication service providers (CSPs) operate in a highly regulated environment, processing highly sensitive subscriber usage data, which leads to enhanced data privacy concerns. Often these concerns are accompanied by misconceptions that regulated data cannot be transferred out of the country or into the public cloud.

In this whitepaper, we will explore data sovereignty regulations with examples from different legislations around the world. Data protection authorities across the globe recognize they need to create a balance between making the public cloud accessible, while moderating data privacy concerns. Their interest is to provide options for international data flows that are viable for the global economy while ensuring the protection of personal data.

Data laws are changing

Data regulations are on the agendas of government authorities worldwide, as they begin to consider the exponential increase in data flow and the significance for overall economies. As a result, many countries are changing their compliance programs.



ECUADOR, with its recent Data Protection Law (available [here](#), in Spanish only), now allows international data transfer to other countries, assuming those countries provide “adequate levels,” or a minimum level of prescribed protection defined by the Ecuador data regulation authority.



MALAYSIA has issued a [Public Consultation Paper](#) about its proposal to remove the whitelist provision from its Data Protection Act. The paper notes that transferring data outside of Malaysia is **essential** to free trade agreements and that a whitelist provision seems to curb data transfers.



INDONESIA proposed a new Data Protection Bill (only available in Indonesian, [here](#)) removes the requirement to notify authorities when enterprises plan to internationally transfer data.

More data protection authorities are allowing data transfer

Globally, data protection authorities are providing different options and exemptions for international data transfer that allow telcos to comply with data regulations. Most countries now enable international data transfer to a select group of countries, where that list intersects with hyperscalers' (AWS, Azure, GCP) data centers in 31 (and growing) countries worldwide. For example, Israel has no hyperscaler data centers of its own yet, but allows data to be transferred to Germany, which has AWS, Azure and GCP data centers.

Today, the rules vary based on country. Since hyperscalers let you specify where your data resides and how you can encrypt your data at motion or at rest, **almost every country can use the public cloud.**

Hyperscalers allow telcos to specify *where their data resides and how they can encrypt their data at motion or at rest in the public cloud.*

Globally, data protection authorities *provide different options and exemptions for international data transfer.*

Most countries allow data to be transferred to a preapproved group of countries

Although different data protection authorities have different regulations, the European Union's General Data Protection Regulation (GDPR) is a well-known one that leads the way for many other countries. According to GDPR, the European Commission may declare a third country as offering an adequate level of protection (known as the "Adequacy Decision"), meaning that data can be transferred to that third country without the data exporter being subject to additional conditions. European Union countries can transfer data to each other and to the other preapproved countries, such as: Andorra, Argentina, Japan, New Zealand, Switzerland, Uruguay, etc., without being required to provide further safeguards or being subject to additional conditions.

GDPR has inspired new data privacy legislation worldwide and has been adopted by many other countries with minor revisions. For example, Argentina, Bahrain, Botswana, Brasil, Chile, Canada, Colombia, Israel, Kenya, Mauritius, Nigeria, Qatar, South Africa, Japan, New Zealand, South Korea, Thailand, Uganda, Uruguay and others have GDPR-like data regulations. To verify whether international data transfer is allowed in your country, check the countries that have been preapproved by your local data protection authority.

GDPR has inspired **data privacy legislation worldwide** and the approach has been adopted by many other countries

ARGENTINA

For example, while Argentina does not have a hyperscaler region within the country, the following countries are approved for data transfer:

- ⚡ EU and the European Economic Area countries
- ⚡ Jersey
- ⚡ Andorra
- ⚡ Switzerland
- ⚡ Isle of Man
- ⚡ Uruguay
- ⚡ Guernsey
- ⚡ Faroe Islands
- ⚡ UK
- ⚡ Canada
- ⚡ Ireland
- ⚡ New Zealand

Therefore, a telecom operator in Argentina can intersect this country list with the list of countries where hyperscaler data centers exist. They could use AWS, Azure, or GCP locations in Canada, Germany, or UK, AWS or Azure locations in France, Italy or Ireland, Azure or Google Cloud locations in Netherlands or Poland.

COLOMBIA

Similarly, Colombia recognizes the following countries as adequate for international transfer of personal data:

- ⚡ EU and the EEA member states
- ⚡ Guernsey
- ⚡ Perú
- ⚡ Andorra
- ⚡ Ireland
- ⚡ Republic of Korea
- ⚡ Albania
- ⚡ Israel
- ⚡ Serbia
- ⚡ Argentina
- ⚡ Isle of Man
- ⚡ Switzerland
- ⚡ Canada
- ⚡ Japan
- ⚡ United States
- ⚡ Costa Rica
- ⚡ Jersey
- ⚡ UK
- ⚡ Faroe Islands
- ⚡ Mexico
- ⚡ Uruguay
- ⚡ New Zealand

Intersecting this list with the list of hyperscaler data centers, a telecom operator in Colombia can use the public cloud data centers of AWS, Azure or GCP in Canada or US, and Azure locations in Mexico.

ISRAEL

Israel, as mentioned above, also has none of its own hyperscaler data centers to-date, but recognizes the following countries as providing adequate protection:

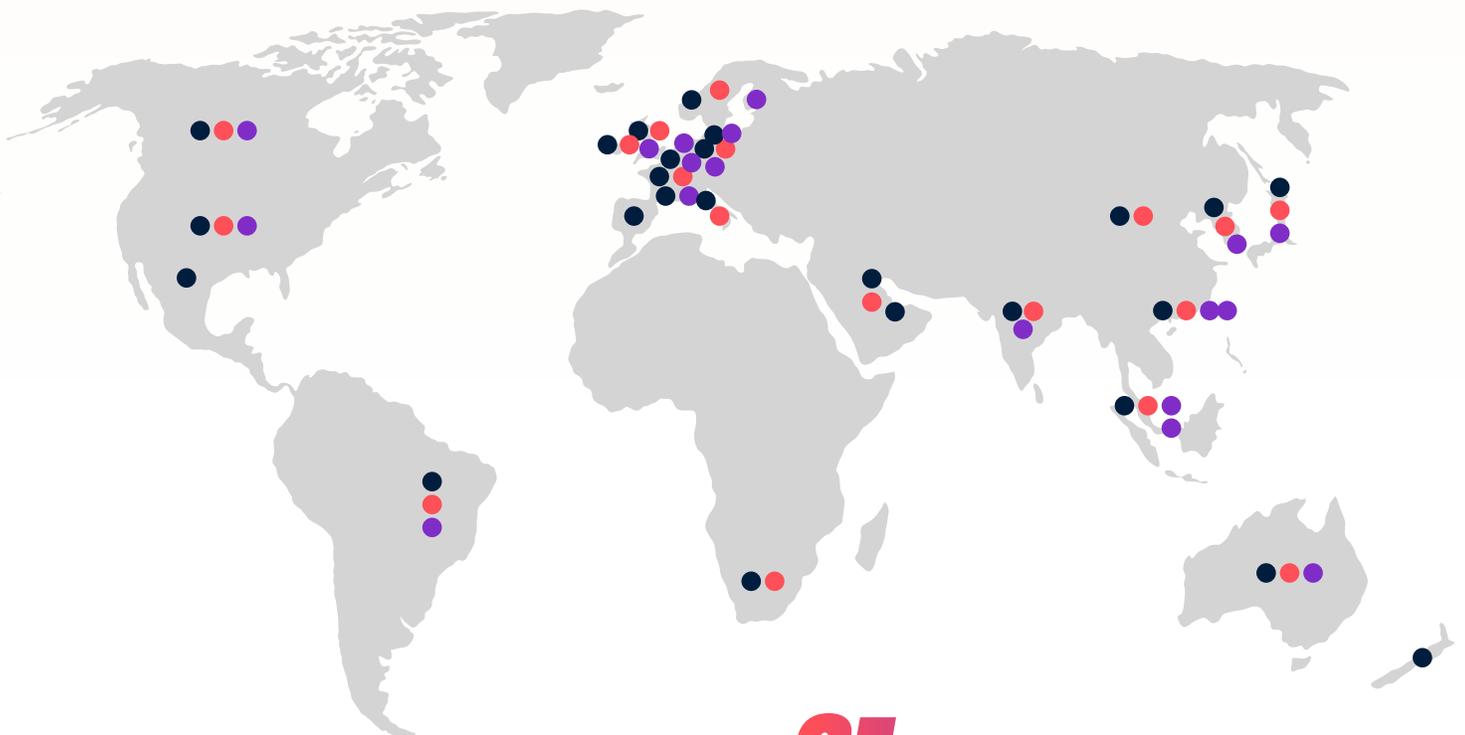
- ⚡ EU and the EEA member states
- ⚡ Guernsey
- ⚡ Jersey
- ⚡ Andorra
- ⚡ Ireland
- ⚡ New Zealand
- ⚡ Argentina
- ⚡ Israel
- ⚡ Switzerland
- ⚡ Canada
- ⚡ Isle of Man
- ⚡ Uruguay
- ⚡ Faroe Islands
- ⚡ Japan
- ⚡ UK

Similarly, a telecom operator in Israel can use the public cloud located in AWS or Azure locations in France, Italy or Ireland, Azure or GCP locations in Netherlands or Poland until both Azure and AWS open their new data center locations in Israel soon.

MAP

Current locations of hyperscalers' data centers

AWS, Azure and GCP currently have data centers in 31 countries—and the list continues to expand. There may be already facilities that will comply with your country's data regulations.



31 COUNTRIES
+ MORE ON THE WAY

● Azure ● AWS ● GCP

Other options

CONTRACTUAL CLAUSES

In some countries, standard contractual clauses that have been preapproved by the data protection authority can be used as a ground for international data transfers to different countries as appropriate data protection safeguards. This works well for destination countries where the laws ensure adequate levels of protection for personal data.

For example, hyperscalers offer a data transfer contract which applies globally and includes contractual commitments to adequately address the obligations of each party for the privacy of data. Case in point: [The Data Processing Addendum of AWS](#) includes standard contractual clauses and gives customers the assurance that AWS will provide all customer data the same level of security, privacy and protection that it provides in the EU. Telecom operators can use it as an appropriate safeguard in EU countries, Serbia or the UK to transfer data to a public cloud location in another country that is not approved. For example, [Telefonica Spain states in its privacy policy](#) that when international transfers are necessary, they will take the necessary organizational, technical and contractual measures to ensure the protection and security of the data, such as, for example, signing the European Commission's Standard Contractual Clauses with the authorized subcontractor or third party recipient. In this way, organizations take on the responsibility of data regulations with a contractual clause, allowing them to use the public cloud more freely.

Similar to the EU, Serbia and UK, the Association of Southeast Asian Nations (ASEAN) recently approved the Model Contractual Clauses for cross-border data flows. The Model Contractual Clauses are a set of recommended contractual provisions that organizations can voluntarily choose to incorporate in relation to cross-border

CONTRACTUAL CLAUSES (Continued)

data transfers in the ASEAN region. ASEAN countries are: Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam. The clauses are used to ensure that the data transferred from one ASEAN jurisdiction to another, for example to any of the hyperscalers' data center locations in Singapore, will continue to be processed in accordance with the data protection laws that apply in the originated ASEAN jurisdiction.

SUBMISSION- BASED BINDING CONTRACTS AND LICENSES

In some other countries, submission-based binding contracts can be used for international data transfers. Submission-based binding contracts are data protection policies that are considered to be the "gold standard" for international data transfers because they provide legal certainty. In such cases, companies are required to submit binding contracts for the approval of the data protection authority. For example, telcos may apply to the authority to get "approved Binding Corporate Rules" to transfer data within the same multinational group, like [BT and Deutsche Telekom](#) did in the EU to transfer data outside the EU.

Submission-based binding contracts can be used to transfer data to international third-party companies in some countries. For example, although Turkey has an article for adequacy decision in its own GDPR, it does not recognize any countries as adequate yet. The data protection authority requires companies to apply for the approval of submission-based binding contracts as safeguards for international data transfers.

In Morocco and Tunisia, international data transfers require prior authorization from the data protection authority. Similarly, in Egypt, transferring personal data is subject to obtaining a license from the authority. For example, Egypt's National Telecom Regulatory Authority has granted BT Group – Egypt a license that allows the company to provide connectivity services and data transfer to business clients operating in Egypt and their branches abroad through its international networks.

Companies can use submission-based binding contracts or licenses to transfer data to another country even if there is no adequacy decision for that country.

Five steps to ensure data regulation compliance

Follow these steps to learn how to comply with applicable data regulations for the countries where you operate:

- 1 Check the regulations** that apply in the countries where you operate. We find the [OneTrust DataGuidance™ tool](#) to be a handy reference. Note that in some countries there are specific rules for telecommunications data.
- 2 Read how the hyperscalers—[AWS](#), [Azure](#), [GCP](#)—address** different privacy and security issues. In particular, make sure to check the certification pages for each one: [AWS](#), [Azure](#) and [GCP](#).
- 3 Understand how you can specify** where your data resides and how you can encrypt your data at motion or at rest here: [AWS](#), [Azure](#) and [GCP](#).
- 4 Check where the [AWS](#), [Azure](#) and [GCP](#) data centers are located** and see if there is one in your country, or in a location where you are able to host your data.
- 5** If you cannot find a suitable hyperscaler data center in which to host your data, another approach is to **see if your local data protection authority allows** you to use preapproved contractual clauses or submit requests for approval to use the public cloud.

CONCLUSION

Public cloud can be used by telcos

30+

telecom operators have already started moving some of their IT stack from their on-premise data centers to the public cloud

Public cloud is designed to deliver secure, high-performing, resilient and efficient infrastructure for different applications. Totogi leverages this design to provide telcos a secure environment for business-critical workloads while meeting their local compliance requirements. All data flowing across the global public cloud network that interconnects the data centers is automatically encrypted at the physical layer. Telecom operators always own their data on the public cloud with the authority to decide the country it is stored in, to encrypt it and move it. They can control the format, structure and security of their content, including whether it is masked, anonymized or encrypted. They can manage their own encryption keys, or use a third party encryption mechanism of their own choice.

More than thirty telecom operators have already started moving some of their IT stack from their on-premise data centers to the public cloud. AT&T, Verizon, [Deutsche Telekom](#), ThreeUK, Telefonica, Telecom Italy, [Vodafone](#), Orange, Truphone Australia, [Globe Telecom](#) Philippines, [Axiata Malaysia](#), KDDI, [Etisalat](#), Telkomsel Indonesia, Zain Iraq and Liberty Latin America are some examples.

Start embracing the full functionality of public cloud like many of the world's biggest telcos already do. Don't give up on the great flexibility, scalability, revenue and cost-saving potential of the public cloud because of preconceived notions about data regulations. Do your research and start your move!

**This whitepaper is provided solely for informational purposes. It is not legal advice, and should not be relied on as legal advice. Each country has its own regulations, please seek adequate legal counsel.*



About Totogi

Totogi is completely redefining how carriers engage subscribers to drive customer love! Our software products – Totogi Charging System and Totogi API Platform – are 100% purpose-built for the public cloud and deliver unparalleled performance and value at an unbeatable, usage-based price (there's even a FREE TIER!).

Learn more at totogi.com »