The CIO's Quest for Compliance

AVOID THE REGULATORY PITFALLS OF CORPORATE COMMUNICATION

bandwidth

TABLE OF CONTENTS

INTRODUCTION

Communication is key in today's business landscape, and modern technology has changed the way we communicate on an international scale.

If you're like every other company out there looking to succeed in the globalized economy, ensuring your business communications remain fully compliant is the only way to guarantee quality, consistency and long-term stability of service. Comms compliance is an area that is often overlooked in the early stages of planning a business strategy, but is an area that can quickly spiral out of control for CIOs and IT managers looking to scale their business while cutting down their snowballing communication bills. CIOs already have a full plate, from managing teams and implementing new technologies to strategic planning and process improvements — but ensuring that communications are compliant needs to be near the top of their priorities, especially given that Gartner estimates communication services are one of the top-three costs for IT.

Being able to comply in a direct way with a short approval time and a user-friendly tool sounds like a dream, but today's telecom providers should make it simple for companies to comply with regulations around the world in a timely manner. The move to global enterprise compounds the issue of compliance because the regulatory landscape varies in every country. It's important to choose vendors that can help you navigate these different terrains. Business comms compliance comes with a unique set of challenges, and navigating through the tangled regulatory web that exists within the communications space requires a significant amount of legal expertise. Without the proper knowledge in place, a dull regulatory headache can quickly develop into a full-blown global compliance migraine, but CIOs can ease the pain by moving away from traditional telephony services and adopting a Communications as a Service, CaaS, provider that makes it easy to comply with regulations in every location they do business.

CHALLENGE:

International Expansion

Scaling your business to a new market is no small feat and the challenge of doing so to multiple disparate markets around the world is even more complicated. This type of expansion is not only exciting, it can also provide several advantages — but from currency fluctuations and tax laws to culture fit, employment regulations and the availability of local infrastructure, each new location comes with countless hurdles even the most capable and agile companies have to jump over.

Yes, international expansion leads to better global presence and growth in demand, but extending your footprint can also result in the headache of compliance regulations — a headache often presented in complex legalase and foreign languages. Businesses should be concerned with regulatory compliance, no matter the country or language. You will find yourself facing a fresh set of challenges in your efforts to establish a local presence for each new market, and you should assess all telecom compliance components before planning to grow your business.

Monitoring

It takes a great deal of preparation and investment for an organization to create a sustainable presence in a new territory, and talk of business communications should be at the heart of any strategic growth planning. Few companies take the time to properly consider how business telephony regulations differ between countries. Today, corporate telephony comprises two-way calling between SIP and PSTN endpoints from all manner of local, national, mobile and toll-free lines, as well as the need for on-premise dialing access to local emergency services – and all of these different facets have their own regulatory considerations. This is without even entering the realm of using different vendors in each market and the exponential increase in contracts and billing that such an approach necessitates. Very quickly, ensuring your communications are compliant becomes a full-time job in itself.

Regulators are starting to migrate away from paper forms in favor of electronic applications, but it can still be an onerous process to monitor and understand the complexities of each market. But, CIOs can't slack on monitoring the status of their contracts if they want to stay compliant. Instead of hiring a team of legal professionals to handle each vendor and contract, consider consolidating your communication services. Find a vendor that delivers the fully compliant communications services you need to stay in touch while also informing you of any changes to the regulatory landscape and advising on steps you might need to take to ensure you stay within the rules.

Regulatory Audits

If your organization is operating in multiple territories, ensuring your communications stay on the right side of all the relevant local regulations can quickly become a burden. But, just as there are serious implications for failing to comply with local employment, corporate and tax laws when scaling your company, the same is also true of your business comms. From registering an end user address within the area code of the requested phone number in Germany to providing a utility bill for registering a geographic number in South Korea, regulation requirements can vary dramatically from one territory to the next. If you fail to comply or opt for vendors operating so-called 'grey routing' into these countries, you could quickly find your lines of communication to customers and colleagues shut down.

Companies are liable to be audited to ensure they remain fully compliant with regulations. In order to avoid consequences and backlash, it's vital your partner helps you understand the various regulations in a given country. While it remains your responsibility to file the appropriate paperwork, a knowledgeable vendor that truly understands the rules can help you untangle and maintain compliance.

Emergency Calls

Calling for help in an emergency is often taken for granted as something that is just there if we need it. Providing on-premise access to local emergency services is required by the FCC in the US, as well as other regulatory bodies around the world. But as you migrate your communications services into the cloud and away from the PSTN, it is important to understand that this is not something every provider can accommodate. Indeed, providing the ability to link a SIP-based phone line to the correct local public safety answering point becomes a valuable service in its own right for the enterprise.

Despite both the US and Europe requiring carriers to provide access to emergency services, the exact specifics of the requirements vary based on location. To remain compliant, most organizations still opt for a landline, but that comes with its own complexities. Having a hard time keeping up with the different requirements? Understandable.

Regulations are constantly changing and your organization must adhere to each country's communications criteria. In the US alone, there is a surprisingly large amount of legislation governing emergency number access, from Kari's Law to the FCC's VoIP E911 Regulations and dispatchable location requirements for wireless

providers. Legislation regulating 911 services provided by enterprise telephony also varies dramatically by state. Expanding your horizon to include international markets only further complicates the picture.

Unless there is a designated role for compliance in each territory, it's impossible for employees to keep all regulations, from each location, top of mind. As a CIO, it's crucial to have access and capabilities that span globally. So, don't install one, or even 100, fixed-line phones for emergencies. Instead, work with a provider that offers compliant phone access to local emergency services in every country where you need it.

To say there is a tangled web of global communications regulations is something of an understatement, but the benefits of the cloud are there for all to see. Many businesses looking to globally scale their operations want to do so rapidly, but traditional telecoms providers can't keep up with the fast-paced demand of modern companies. Scaling in a manner that is rapid and cost-effective is one area where cloud communications really excel. Every CIO knows they need to be compliant, but there are ways to streamline this process so it's not a constant headache. The truth is, global domination requires a compliant, international reach, and enterprises can only do that with the right provider. So, when it comes to your quest to establish your business in new markets, choose a communications provider painstakingly dedicated to taking the complexity out of global business communications by helping you to solve as many of these challenges as possible.

CHALLENGE:

The Contact Center

Customer service has moved into the digital age and modernized the way contact center agents deliver support, whether through voice, email, chat, SMS, social or mobile. Organizations demand a provider that can deliver communications services built to fulfill the needs of contact center managers servicing the high expectations of today's customers.

This isn't shocking considering better customer experience (CX) and creating a unified cross-channel view of customers are some of the major focuses of digital transformation initiatives. A contact center is a great tool to improve satisfaction, reduce churn and increase average revenue per user. Do you see the common denominator? These are all key metrics for as-a-service businesses in particular. It's a strategy digital-native companies are using and one which all businesses should mimic as part of their digital transformation initiatives.

Take this agile car manufacturer as an example: They wanted to enter a few new markets and posted information on their website about the additional locations, including a toll-free number for people to call. Based on which markets generated the most calls, the manufacturer was able to decide where next to deploy commercial operations. As a result, the company was able to wait until after customer acquisition to enter the market, then dynamically scale operations in real time.

To achieve this level of agility, the company required a communications provider that is fully engaged with the regulatory landscape in each market and able to help streamline the process of ensuring compliance as they scaled their contact center With fully compliant toll-free phone numbers in each country routing calls to a centralized contact center, this manufacturer has an extremely low-cost way of measuring opportunity in various new markets and even to start selling cars before local physical operations such as showrooms have been established. Their only cost is maintaining a SIP-powered toll-free number in each country.

Compliance is essential for long-term service stability of voice and messaging services. When it comes to dealing with customers directly, it's important to go the extra mile to make sure you don't miss a beat when it comes to privacy protection compliance and best practices.

Customer Privacy (GDPR)

Achieving full General Data Protection Regulation (GDPR) compliance shouldn't be guesswork. If your organization determines the processing or storage of your users' personal data, then you are considered a "Controller." If you store or process the personal data for another business, then you are a "Processor." Some businesses fall into one or the other category, and some meet the criteria for both.

Here is a checklist of some of the main points to consider when navigating GDPR:

✓ Obtain customer consent

Ensure you have a legal ground for collecting and processing your customer data, whether by form of consent or legitimate grounds etc. The GDPR requires you to obtain customer consent before you store or process their data. You must explicitly request consent and receive it in concrete and provable terms.

✓ Appoint a Data Protection Officer (DPO)

Having a DPO is not only a good way to ensure compliance, but it's also a standard. Among other duties, they will perform regular monitoring of data storage and processing on a large scale.

✓ Perform a Data Protection Impact Assessment (DPIA)

Each product, service or project involving a customer's personal data should begin with a DPIA. This is an audit of procedures and processes to quantify how they will affect the customer's privacy and ensure that that privacy is in mind from the very outset.

✓ Send Out Alerts After Any Data Breach

While everyone does their best to protect their own and their customers' personal data, hostile actors are always a threat. You must sound the alarm after any hostile data breach. This is done to speed the customer's recovery and to help others avoid any remaining hazard.

✓ Minimize the amount of data you store

The GDPR data minimization principle helps ensure that only useful and relevant data is collected, processed or stored. The aim is to ensure that you are only using personal data that is absolutely necessary in order to perform the service or task at hand.

✓ Respect the Customer's Right To Be Forgotten

This is a privacy policy that is designed to let people grow, and not be hindered by old work that they no longer wish to be associated with. It provides the mechanism by which an individual can request for their personal data to be deleted.

Even for US-based businesses, it is mandatory to adhere to GDPR standards for their European customer base. It is also crucial to consider other national requirements and sector-specific legislation around data protection and security.

Customer Expectation When Contacting a Vendor

Balancing the need to deliver top-notch customer service while protecting privacy needs can be a challenge. It can require some level of forbearance and cooperation on the part of your customer. As the vendor, your best bet is to make sure your clients and customers understand at the earliest possible point how they can help secure their privacy during service calls.

Customer Service and Quality Customer Experience

The call center staff and their systems should make every effort to secure the information given by the customer and delete any and all irrelevant information.

✔ Using Text

Verifying a customer's identity using text is a great way to ensure privacy. Texts are automatically encrypted on both ends and can be used to send temporary verification codes by the user. SMS-enabled numbers are a prerequisite for this type of service.

✔ Domestic calls

Consumers are 34 percent more likely to want to learn more about the product or service from sales calls with a local phone number. Not only does dialing from a local number create better response rates and bring a large business closer to home for customers, but it also limits the opportunity for hackers to access user data from undisclosed locations and helps you provide better customer service because call traffic is not routed internationally.

By using both text verification and local outbound calling, your business can scale dramatically in real time, while never missing a beat in terms of protecting your customers' privacy and remaining safely within regulatory guidelines.

CHALLENGE:

Corporate Telephony

In 2019, the emphasis placed by CIOs on corporate communications is only set to grow. Gartner projects that worldwide IT spending will rise by 3.2% to $3.8 trillion this year, with communications services accounting for nearly 40% of this figure – an increase of 1.2% for the category compared to 2018. With so much on the line, it's crucial for CIOs and IT managers to ensure the fundamental building blocks are in place and up to standard for their platforms and overlying communications services. While they may have KPIs around the push for cutting-edge technologies and improvement of services, ultimate judgment of success is still reserved, in most cases, for more foundational goals such as ensuring accessibility to, and continuity of, services.

Network Dependability and BCDR

For communications, this means ensuring the network underlying your voice and messaging services can provide enterprise-grade dependability in terms of redundancy and failover mechanisms that align with your own Business Continuity and Disaster Recovery (BCDR) processes, while the services themselves must be fully compliant with all relevant regulations to ensure long-term availability. This will be critical to your ability to deliver on any internal SLAs around uptime and service availability.

Such dependability requires multiple layers of redundancy from communications service providers, with automatic failover mechanisms for hardware such as access points and gateways, critical systems, network paths, datacenter connections and signaling proxies.

Information Security

On top of this, there are very real considerations around information security that CIOs need to keep top of mind. First and foremost, calls and call patterns should be fully secure and not logged anywhere external to your own platform or–and only if required–the platform of your communications provider.

Data Retention

It is imperative for CIOs to make sure their enterprises are in compliance with national data retention schemes, which can vary from country to country. For Call

Detail Records (CDRs), this usually entails storing non-anonymized records of calls for a period of time set by the national regulator in a given country, then ensuring these records are anonymized after that time period has passed in order to comply with provisions such as those set out by the EU's General Data Protection Regulation (GDPR) in Europe.

In a growing list of countries, particularly within the EU, law enforcement authorities will demand that communications vendors provide electronic access to end user details for phone lines. The onus is on you to share this information with your vendors. For example, the Department of Public Security's Data Processing Center in Italy has created a computerized National Telephone Directory system (called ETNA) for authorized law enforcement inquiries.

While reputable communications providers will observe and obey all such regulations, it is crucial CIOs understand the responsibility of regulatory compliance remains solely with their enterprise. It cannot be offloaded to third-party providers, even if they can help explain and streamline the processes of providing regulators and authorities with relevant end user information.

Call Security

Ensuring that the signaling and the media of the calls themselves are secure requires three separate layers of encryption:

1 TLS

Transport Layer Security encrypts the signaling traffic of the call itself. In other words, call metadata and things such as DTMF tones that might be required by a bank asking an end user to verify their account details.

2 SRTP

Secure Real-Time Transport Protocol encrypts the payload, or the part of the transmitted data that makes up the intended message. In the case of phone calls, this is the actual speech traffic.

3 VPN

Virtual Private Networks extend your private corporate network across the internet by creating secure encrypted tunnels in situations where you need control over traffic streams or direct connectivity doesn't make cost sense, such as when serving sparse support locations.

Handling of Sensitive Data

For many industries, there will be additional regulations around the handling of sensitive data to which communications services must adhere. For example, the Payment Card Industry Data Security Standard (PCI DSS) sets out specific controls for organizations handling credit card information. Similarly, the Health Insurance Portability and Accountability Act (HIPAA) is enacted in the US to ensure that there are established procedures including authorization and request functions for the storing and sharing of identifiable patient information.

Information privacy laws and frameworks such as these extend to the content of voice and text communications between organizations and their end users. CIOs in industries such as banking and healthcare must always ensure their communications providers are adhering to any such additional regulatory frameworks and this will be a component of the decision when choosing between vendors.

Activation of Numbers and Services

Once you have a provider in place that adheres to any relevant data standards and offers both network dependability and BCDR, the regulatory focus shifts to the activation of the voice and messaging services themselves. Communications technologies must enable the enterprise telephony system's end users to communicate to the rest of an organization and also externally to the rest of the world.

Because a company's workforce is not a static thing – people come and go and move to different roles within an organization – CIOs need a platform that can instantly provide phone numbers so they don't need to plan ahead when it comes to the number of business seats they will need. After all, along with email, a phone number is one of the main identifiers for a corporate employee.

For this reason, instant access to phone numbers is important. Aside from the technical requirements inherent in the delivery of on-demand service, there are also compliance demands that must be considered. Because regulators in many countries will have local address requirements, meaning that businesses must register an address or end user entity for a particular phone number.

This means that phone number inventory needs to be associated to the locations of an organization's end users. The CIO needs to ensure that their enterprise respects fully the local regulations of the country in which a given end user is situated. And so their requirement goes beyond a platform that can instantly provision new numbers

to one that also provides a way of syncing up these HR location registries with this inventory and sharing the necessary information with regulators to streamline the steps required to ensure compliance. Preferably, this functionality will be offered by API so the process can be automated.

Ensuring Continuity of Service

Provision of service has now been established in a way that respects local regulations, but the quest for compliance is not over yet. One of the top KPIs for technical systems is continuity of service and changes to the compliance landscape pose a significant risk of disruption to telephony functions. How do CIOs ensure that their mission-critical communications remain up and running? Beyond the issues we have already considered – network dependability, SLAs, security, redundancy and BCDR – they need to ensure they are aware of changes to the regulatory environment within a specific country.

That means choosing a communications platform with the necessary regulatory expertise in every market to provide advanced notification of any changes to the rules that might impact on continuity of service without some form of action being taken by the enterprise. This ongoing management of compliance needs to be delegated, so the system should have the ability to send alerts to the relevant parties in your organization so that they are aware of new restrictions around voice and messaging services as they are made.

One last consideration is the threat of business telephony misuses cases, whereby an organization is reported upon for claims of unwanted calls that are abusive in nature. These cases might come about as the result of a hack, or an external malicious party spoofing the CLI of their own phone to appear as if it comes from an organization. Think about a typical phishing attack, which might include a phone number purporting to be from a consumer's bank. Abuse cases could also come about as a result of overzealous sales and marketing practices within your organization, resulting in an overabundance of unwanted calls. Whatever the reason, as CIO, you need to be aware that these issues are being brought to the attention of the appropriate parties and ensure that relevant investigations are carried out – whether internally or by your communications provider.