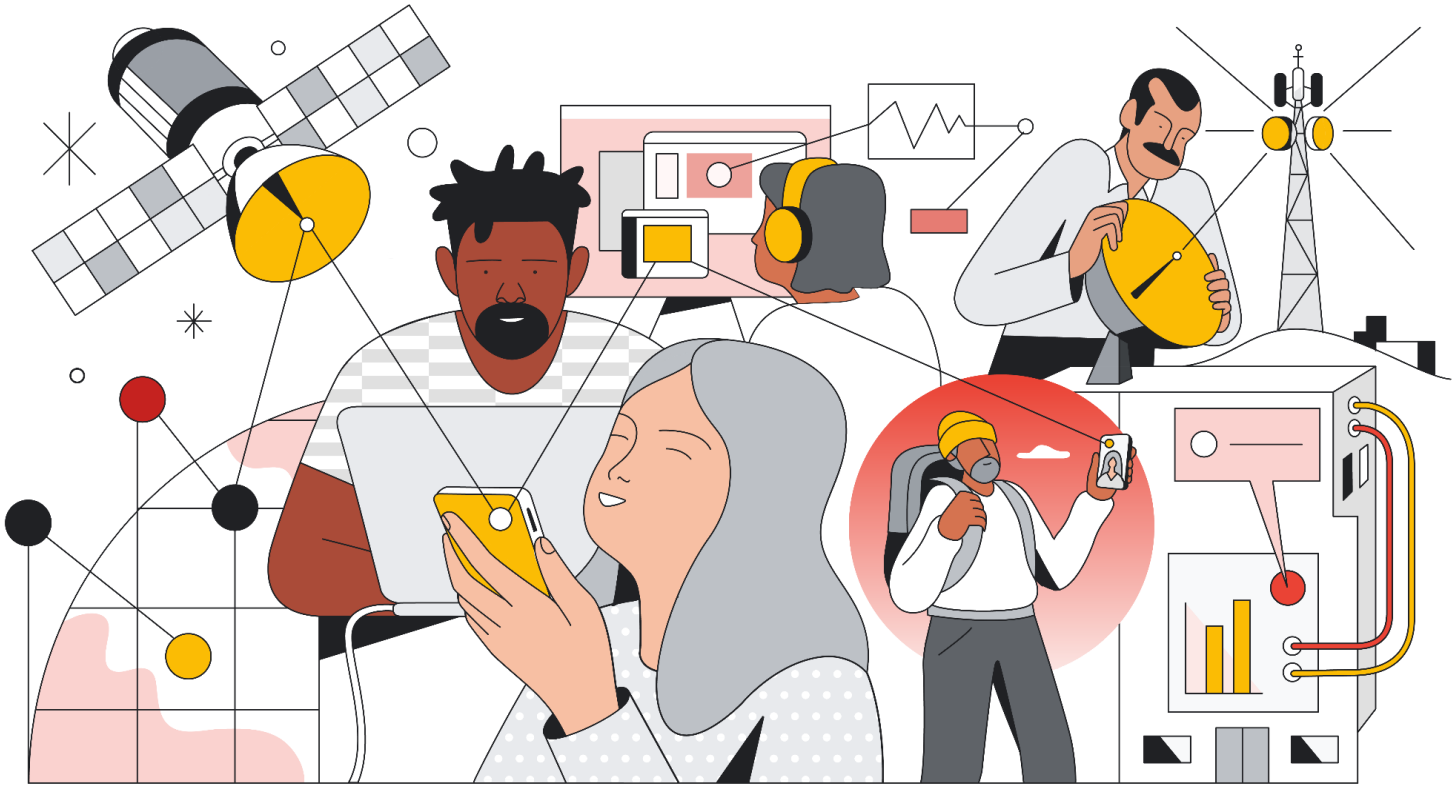
Google Cloud

Google Cloud Whitepaper
September 2023

Insights into Middle Eastern Telecoms Regulations



Disclaimer

This whitepaper applies to Google Cloud products described in the Google Cloud Services Summary. The content contained herein is correct as of September 2023 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Introduction

Telecommunications is perhaps the most significant engine of world economic growth. Telecoms have powered social change and business expansion for almost 200 years, from telegraphs at the dawn of the Industrial Revolution to today's mobile apps, video, and data services. This does not show any signs of slowing down as data consumption is expected to grow by over 400% between 2021 and 2027 in the Middle East and North Africa. It's easy to see why: Communications Service Providers (CSPs), as they are known today, connect people and their inventions, enabling new markets and innovations.

Accordingly, the leaders of Communications Service Providers are looking for innovative ways to unlock new revenue streams, transform the end-to-end customer experience, handle explosive usage, effectively manage increasingly complex systems, unlock the full potential of their data, and deliver on sustainability objectives.

Underpinning these focus areas, Communications Service Providers across the Middle East are focused on ensuring they operate their critical infrastructure in line with ever-evolving regulatory, security, data privacy, and sovereignty requirements. As organizations accelerate their digital transformation journeys towards long-term growth - powered by cloud technology - there is a need to understand both the implications of these regulations for cloud and how the cloud can help Communications Service Providers to address these challenges.

This paper provides:

- An overview of the security and privacy related regulations, guidelines, and standards that apply to Communications Service Providers across the Middle East.
- Insight into the key themes and principles that emerge from the regulations.
- Guidance on how Google Cloud can help Communications Service Providers meet their regulatory requirements.

Regulatory themes

Telecom networks are critical in supporting economic development and national security in the Middle East. CSPs are also trusted with large amounts of sensitive customer information. Therefore, CSPs and the telecoms networks they operate are subject to many security and privacy-related regulations. This includes both global security standards and national-level regulation and guidelines.

A survey of specific regulations affecting CSPs in the Middle East is included in the Appendix. In this section, we summarize the main themes emerging from these regulations and how Google Cloud can help.

Foundational security

CSPs are high-profile targets for cybersecurity attacks and require protection against cybersecurity risks, including state-level and state-sponsored attacks, insider threats, industrial espionage, and sabotage. Increasing cybersecurity concerns have led to governments reevaluating and updating their regulatory frameworks. Many are observing and modeling their updated laws and regulations on internationally recognized security standards, including

- ISO 27001
- ISO 27017,
- ISO 27018,
- AICPA SOC2 (SSAE 18), and more.

Security regulations and guidelines identify many specific security measures and best practices across domains, such as physical security, network security, identity and access management, security incident management, and personnel security.

How we help: Google Cloud has comprehensive and in-depth security controls that we have deployed to help protect your data, summarized in this security overview whitepaper. Other whitepapers detail our security practices in specific areas, including encryption at rest, encryption in transit, and infrastructure security. Beyond our security measures, we also publish guidance on security best practices, use cases, and blueprints.

Google Cloud's security, third-party audits, and certifications help support customer's compliance. Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google Cloud undergoes several independent third-party audits regularly to provide this assurance. Customers can request reports via our Compliance Reports Manager.

Data privacy and communications confidentiality

With consumers entrusting CSPs with large volumes of sensitive customer data, including personally identifiable information and communications records, it's important that the consequences of data breaches be understood.

Protecting customer data privacy and confidentiality of communications are fundamental requirements for telecom operators. Unethical usage of customer data can lead to financial penalties (see Appendix A for more information on specific regulations) and loss of customer trust.

How we help: Google Cloud's trust principles provide a starting point for our approach to data privacy.

Customers own their data, not Google. We want you to feel confident that taking advantage of Google Cloud doesn't require you to compromise on security or control of

your business's data. Google Cloud does not use customer data for advertising and we do not sell customer data to third parties. Our Cloud Data Processing Addendum for Google Cloud further describes our commitment to protecting your data.

Google Cloud is also compliant with international standards on data privacy, such as:

- ISO 27018 (Cloud Privacy)
- ISO 27701 (Privacy - Data Processor)

Additionally, Access Transparency for Google Cloud and Google Workspace supports this trust by providing logs of actions taken by Google staff and the reason for access including references to support tickets where relevant.

For more information, refer to our whitepaper on trusting your data with Google Cloud and to Google Cloud's Privacy Resource Center.

Data residency

The regulatory bodies of Middle Eastern states expect organizations to know where customer data resides. To meet their data residency needs, CSPs in the Middle East look to cloud providers to offer the same level of trust and transparency that their customers demand.

How we help: Google Cloud services offer customers the ability to control where your data is stored via Data Residency. Google will store that customer data at rest only in the selected Region/Multi-Region in accordance with our Service Specific Terms.

In the Middle East, customers can store data at rest exclusively within three cloud regions, Tel Aviv Region Data Center (me-west1), Doha Region Data Center (me-central1), and Dammam Region Data Center (me-central2). We have also announced plans to bring Google Cloud regions to Kuwait as well.

To assist customers in enforcing these controls, Google Cloud offers Organization Policy constraints which can be applied at the organization, folder, or project level. You can limit the physical location of a new resource with the Organization Policy Service resource locations constraint.

Google Cloud customers can use VPC Service Controls to restrict the network locations from which users can access data, defining a service perimeter outside of which customer data cannot be accessed. This functionality allows customers to limit user access by IP address filtering, even if the user is otherwise authorized. Cloud Armor also allows customers to restrict locations from which traffic is allowed to their external load balancer.

Operational requirements

Should the availability of public communication services be impacted by a security incident, widespread disruption could occur. This has potential implications for both public safety and national security. CSPs could also face fines, reputational damage, and loss of business. CSPs are responsible for ensuring they are designing for high availability (as well as security) when planning cloud solutions.

How we help: Google Cloud publishes architecture guidelines to help customers achieve high availability at scale.

Google Cloud also supports customers with Backup and Disaster Recovery solutions. CSPs can use these solutions to design, build, and validate robust disaster recovery patterns that meet their specific recovery time objectives (RTOs) and recovery point objectives (RPOs).

To complement this, Google Cloud also has comprehensive internal plans and systems for its business continuity (refer to ISO 22301).

Google Cloud also offers customers the choice of manual or automated software updates, with the flexibility to control software update approvals and scheduling. Refer to OS Patch Management for an example.

Google Cloud security solutions

In addition to the security features and regulatory compliance already described, Google Cloud offers several Security solutions for a more comprehensive and holistic approach to security.

CSPs migrating to the cloud may not initially have the expertise to decide which security capabilities they need. Security solutions help customers identify those needs and rapidly roll out of relevant security functionality based on common blueprints and established best practices.

Security Foundations solution

As a starting point for customers who need clarification on their security needs, the Security Foundations solution includes a set of recommended products and security capabilities to help CSPs achieve a strong security posture within their Google Cloud environment.

This solution is based on the Security Foundations whitepaper and aligns with Google Cloud's security best practices.

Security and Resilience Framework (SRF) solution

Google Cloud can also support CSPs in carrying out a thorough review of their security practices.The Security and Resilience Framework helps customers to establish or refresh their security program, founded on a risk-based assessment of the entire cybersecurity lifecycle (identify, protect, detect, respond, recover), utilizing established industry frameworks.

The Discovery Platform supports the assessment and includes security maturity assessments across multiple domains. Google Cloud will provide a tailored set of recommendations around security best practices and recommended Google Cloud security products and solutions.

Web App and API Protection (WAAP) solution

The Web App and API Protection solution (WAAP) provides capabilities that protect applications, websites, and public APIs from internet-based threats, including DDOS, fraud, and botnet attacks.

This solution is relevant for all CSPs since DDOS attackers commonly target their infrastructure and systems, and unfortunately, the increased adoption of APIs by CSPs can expose their capabilities. In 2022, Google Cloud successfully identified and blocked the largest DDOS attack on record, demonstrating our ability to protect customers from internet-based attacks.

The WAAP solution includes the following products:

- Cloud Armor
- reCAPTCHA Enterprise
- Apigee API Management

Autonomic Security Operations (ASO) solution

Google Cloud's Autonomic Security Operations solution helps CSPs withstand security attacks through an adaptive, agile, and highly automated approach to threat management.

This solution is relevant for Providers that are interested in transforming their existing Security Operations Centre (SOC) or Security Incident and Event Management (SIEM) by increasing scale, automation, and the use of machine learning (ML) to keep up with a high volume of security incident data and deliver effective threat intelligence and incident response. For more information, refer to our Autonomic Security Operations whitepaper.

Finally, customers can leverage the power of Chronicle and Mandiant, to transform their security operations and achieve a 10X increase in productivity, visibility, and speed.

Conclusion

Communications Service Providers in the Middle East are looking to transform and grow their businesses. Digital transformation initiatives include modernizing core network and IT systems (including operations support system (OSS) and business support system (BSS)) via migration to the cloud and adopting cloud-native architectures. CSPs are also looking to improve customer experience and operational efficiency and monetize their data by adopting cloud-based analytics and ML to gain insights from their customer and network data.

Google Cloud has the tools to help organizations meet their initiatives and compliance needs to drive operational efficiency in information technology, network, and core systems. Google Cloud continues to innovate in areas such as encryption, key management, auditability, transparency, and data residency to help CSPs meet their operational security, resilience, and data privacy needs.

As the industry continues to evolve, we remain committed to keeping in step with laws and regulations, the evolving needs of their customers, and consumer demand in the telecommunications industry.

Appendix A: Regulations and Standards Impacting the Telecom Industry

This appendix contains a survey of relevant global, regional, and national security standards, regulations, and guidelines for Middle Eastern CSPs. This whitepaper is not intended to represent all of the compliance enablement features Google Cloud offers its customers and may not include a summary of all applicable laws.

Global Security Standards

The following global standards on Information Security are not specific to Telecoms but are widely accepted as a baseline for good security practices and provide a way to measure organizational compliance to internationally recognized security policies.

Google Cloud supports compliance with many global standards, including the following:

- ISO 27001 outlines and provides the requirements for an information security management system, specifies a set of best practices and details the security controls that can help manage information risks
- ISO 27017 provides guidelines for information security controls applicable to the provision and use of cloud services
- ISO 27018 relates to one of the most critical components of cloud privacy - the protection of personally identifiable information (PII)
- AICPA SOC2 is based on the Statement of Standards for Attestation Engagements No.18 (SSAE 18).

Refer to the Google Cloud Compliance Resource Center for more information on the above standards, plus many more.

Regional Standards & Initiatives

Euro-Mediterranean Regulators (EMERG)

EMERG is a charter of Europe, Middle East, and North Africa states who share a common interest in regulatory frameworks, including cybersecurity and data protection. The member states primarily border the Mediterranean Sea and span Europe (specifically Austria, Bosnia and Herzegovina, Croatia, Germany, Greece, Italy, Malta, Montenegro, Portugal, Spain, Slovenia, and Switzerland), Middle East (specifically Cyprus, Israel, Jordan, Lebanon, Palestine, and Turkey), and North Africa (specifically Egypt, Libya, Morocco, and Tunisia). The overall objective of EMERG is to either adapt or assimilate EU legislation (such as the EU General Data Protection Regulation - GDPR and EU Cybersecurity Act) into the regulatory framework of Middle East and North Africa (MENA) member states.

Narrowing the focus to the Middle East, three member states have amended their telecommunication laws and regulations to incorporate objectives for data protection and cybersecurity (specifically Cyprus, Israel, and Turkey). The remaining member states have not yet incorporated data protection or cybersecurity objectives into their regulatory frameworks, but they are looking to EU directives as an example. The following Middle Eastern EMERG member states are seeking guidance for updating their telecom regulations:

- Jordan
- Lebanon
- Libya
- Palestine

Gulf Cooperation Council (GCC)

The GCC is a charter of states bordering the Arabian Gulf (specifically Saudi Arabia, Bahrain, Qatar, UAE, Oman, and Kuwait) to facilitate cooperation and communication. One of their primary objectives is to align laws and regulations to ease trade and transfer, including for the telecommunications industry.

National Regulations

Bahrain: Personal Data Protection Law (PDPL)

On August 1, 2019, the "**Law No. 30 of 2018**" (PDPL) came into force in the Kingdom of Bahrain. The PDPL was then further supplemented when the Kingdom's Minister of Justice, Islamic Affairs, and Waqf issued 10 additional resolutions aligning the PDPL more closely with international standards.

Bahrain: Telecommunications Law

On October 23, 2002, the Kingdom of Bahrain enacted the "**Law No. 48 of 2002**" (Telecommunications Law) to establish a regulatory framework for the telecom sector. The law establishes limited requirements for telecom operators to maintain data and communication privacy with the "**Article 3(b)(1).**"

Cyprus: Law 125(I) of 2018

The Republic of Cyprus is both a Middle East and an EU member state, so they are subject to the **EU General Data Protection Regulation (EU) 2016/679**. Cyprus passed the "**Law 125(I) of 2018**" (Law providing for the protection regarding processing of personal data and for the free movement of such data) to supplement the GDPR and established the Office of the Commissioner for Personal Data Protection as the supervisory authority in Cyprus.

How we help: We support your organization's efforts to improve customer security and privacy with our GDPR compliance capabilities. As a data processor who processes data on behalf of the data controller, we have clearly laid out our terms of business that reflect Article

28 requirements. These terms include data protection, security, data retention and deletion per our Cloud Data Processing Addendum. Please visit our Compliance Resource Center to learn more about the certifications and compliance standards that we satisfy.

Israel: Protection of Privacy Law (PPL)

The PPL and its implementing regulations govern the collection, use, disclosure and other processing of personal data (including sensitive personal data) in Israel by public and private entities and provides data subjects with rights over their personal data. The Privacy Protection Authority ("PPA"), through its statutory power as the Registrar of Databases, supervises compliance of private and public entities with the PPL and all regulations thereunder, including the Privacy Protection Regulations (Information Security) ("Security Regulations"), and the Privacy Protection (Transfer of Data to Databases Abroad) Regulations, 5761-2001 ("Transfer Regulations"). The PPA regularly publishes guidance materials, including Q&A and additional guidance with respect to the Security Regulations, as well as guidance on the use of outsourcing services for processing personal information and the responsibilities of Data Protection Officers. In addition to its administrative and criminal investigatory powers, the PPA is granted with authority to impose administrative fines in certain circumstances.

How we help: We have created a whitepaper intended to help our customers understand the PPL, Security Regulations, and Transfer Regulations and how Google Cloud implements data privacy and security capabilities to store, process, maintain, and secure customer data in a way that aids customers in meeting their regulatory obligations.

Israel: Telecommunications Law

The State of Israel passed the "**Telecommunications Law**" (5742-1982) to establish the regulatory framework for communications and broadcasting. The law establishes some cybersecurity and data privacy objectives including the "**Article 29. Impairing a Telecommunications Facility**", "**Article 30A. Transmission of an Advertisement through a Telecommunications**" [sic], and more.

Kuwait: Data Privacy Protection Regulation

At present, the State of Kuwait does not have general data privacy and protection laws. However, the telecom regulatory authority, Communication and Information Technology Regulatory Authority (CITRA), enacted the "**Regulation No.42 of 2021**" (Data Privacy Protection Regulation) to introduce a regulatory framework necessary to establish objectives in data protection and cybersecurity.

As previously mentioned, the Kuwait communication and information technology regulatory framework does not currently contain objectives for general data privacy and protection. The framework also does not contain objectives for cybersecurity. The Ministry of Communication (MOC) has published a list of laws and general guidance, but the actual text of the laws are largely maintained internally. However, the "**Law No. 37 of 2014**" (Establishment of CITRA)

highlights the responsibilities of CITRA based on the MOC laws, among others (such as laws regarding penal codes, GCC treaties, union agreements, etc.).

Oman: Personal Data Protection Law (PDPL)

The Sultanate of Oman issued the "**Royal Decree NO 6/2022**" (PDPL) in February 2022, which came into force on February 13, 2023. The PDPL strengthens existing data privacy and protection laws, including new fines for a breach where personal data is compromised.

Qatar: Personal Data Privacy Protection Law (PDPPL)

In 2017, the "**Law No.13 of 2016**" (PDPPL) was enacted in Qatar and became the first regulatory framework for data privacy and protection among GCC member states. The regulatory body which oversees the law is the Compliance and Data Protection authority (CDP), and the CDP has published guidelines, accreditation, and certification necessary to comply with the law.

Qatar: Telecommunications Law

The State of Qatar enacted the "**Law No. 34 of 2006**" (Telecommunications Law) in 2006 with primary objectives promoting the growth and transformation of telecom operators and consumer protection and transparency. The "**Chapter 16**" does outline the importance of security of critical infrastructure, including cybersecurity (such as penalties for cybercrimes).

Qatar National Information Assurance (NIA)

Qatar National Cyber Security Agency (NCSA) approved National Information Assurance (NIA) policy is a comprehensive framework based on the best practices of leading organizations and international standards. It is designed to guide organizations in implementing effective information security controls. The NIA policy assists organizations in protecting their information assets, managing risks, complying with regulations, and achieving international standard certifications. NCSA requires a third-party assessment of any organization interested in being certified against the NIA policy. The robust certification process requires that a third party assess a cloud provider's security controls and compliance with Qatari laws and regulations.

How we help: Google Cloud has obtained Qatar's NIA certification through an accredited third-party assessment organization that has attested that Google Cloud meets the highest Qatari security and compliance standards.

Saudi Arabia: Personal Data Protection Law (PDPL)

On September 17, 2021, the Kingdom of Saudi Arabia passed the "**Royal Decree M/19**" (PDPL), and the law will come into force on September 14 , 2023 and will have a one year grace period. The SDAIA has also released corresponding Implementing Regulations and regulations on cross-border data transfers. The Implementing Regulations and the Regulations on

Cross-Border Data Flow have since been released for public consultation and will enter into force as well on 14 September 2023 with a one year grace period alongside the PDPL

To facilitate the PDPL, Saudi Arabia enacted the "**Royal Decree No. M/106**" (Telecommunications and Information Technology Act) on December 7, 2022, which is overseen by the Communications & Information Technology Commission (CITC)[1]. The updated law replaces the original Telecommunications and Information Technology Act from June 4, 2001. The Royal Decree No. M/106 establishes objectives to focus on new and emerging technologies and a renewed focus on cybersecurity and data protection.

Türkiye: Electronic Communication Law and Personal Data Protection Law (PDPL)

The Republic of Türkiye (Turkey) had objectives for some cybersecurity and data privacy in the "**Law No. 5809**" (Electronic Communication Law) which entered into force on November 5, 2008. However, Turkey is a party to the "**Treaty 108**" (Convention for the Protection of Individuals with regard to Automated Processing of Personal Data of 1981) which requires that personal data privacy is recognized as a fundamental right, and the Electronic Communication Law does not establish this objective. To align with the treaty, Turkey established personal data privacy as a fundamental right with the "**Law No. 6698**" (PDPL) on April 7, 2016, which also strengthened objectives of data protection and cybersecurity.

United Arab Emirates (UAE): Protection of Personal Data Law

The UAE enacted the "**Federal Decree Law No. 45/2021 on the Protection of Personal Data**" on January 2, 2022, to enumerate data privacy as a fundamental right and create a regulatory framework for cybersecurity and data protection. The UAE consulted over 30 major technology companies (such as Google, Microsoft, and Amazon) to ensure personal data is protected on a global basis, including citizen data rights and adequately protected cross border data transfers.

United Arab Emirates (UAE): Telecommunications Regulations

The UAE Telecommunications and Digital Government Regulatory Authority (TDRA) has published all regulations and rulings related to the telecom sector. It is important to note that the telecom sector is a closed duopoly consisting of Etisalat Group (Etisalat) and Emirates Integrated Telecommunications Company (EITC or du). Of particular note is the "**Information Assurance Regulation**" which creates a cybersecurity framework for information technology and telecom providers. It is based on a number of internationally recognized security standards (such as ISO/IEC 27001, NIST 800, and SANS 20). The TDRA requires adherence to the regulation based on criticality. If the TDRA has recognized an entity as critical, that entity must adhere to all security standards, while non-critical entities are strongly urged to adhere to them.

[1] The CITC has since been renamed to the Communications, Space, and Technology (CST) Commission.