Google Cloud Whitepaper
April 2023

Google Cloud

Insights into European Telecoms Regulations

Insights into European 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 April 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. 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.

The industry, however, finds itself in the midst of epic disruption - facing low single-digit revenue growth[1], increasing CAPEX investments and demand on the network, and challenges in customer experience. Accordingly, CSP leaders around the world are looking at 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, CSPs globally are focused on ensuring they operate their critical infrastructure in line with ever-evolving regulatory, security, data privacy, and sovereignty requirements. As CSPs 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 CSPs to address these challenges.

This paper provides:

- An overview of the security-related regulations, guidelines, and standards that apply to CSPs within a European context
- Insight into the key themes and principles that emerge from the regulations
- Guidance on how Google Cloud can help CSPs meet their regulatory requirements

Regulatory themes

European law designates telecom networks as critical infrastructure due to the critical role of communications for all parts of society. 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. In a European context, this includes global security standards and both EU-level and national-level regulation and guidelines.

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

Changing regulatory landscape

The regulatory landscape for CSPs is evolving rapidly due to a changing world with new and emerging security threats, geopolitical power changes, and socio-technological changes such as mass digitisation, cloudification, and software-based networks - providing a stimulus for regulatory change.

[1] TM Forum, September 2022

CSPs must navigate the regulatory landscape and respond quickly to any changes in laws and regulations. For example, many European nations have recently updated their primary telecoms laws to adopt the European Electronic Communications Code (EECC). Parallel to this, many countries are introducing additional legislation related to cybersecurity and national resilience (e.g., the Electronic Communications Security Measures Regulation and Telecoms Security Code of Practice in the UK). At the time of writing, regulators are also debating the proposed EU Cloud Services Scheme or the EU Cyber Resilience Act.

> **How we help:** Google Cloud monitors ongoing legislation and works closely with regulators (such as ENISA and NCSC) to ensure that data protection and cybersecurity frameworks are fit for both organisational growth and consumer protection. Furthermore, for years, Google Cloud's industry-leading controls, contractual commitments, and accountability tools have helped European organisations meet stringent data protection regulatory requirements. This commitment to supporting the compliance efforts of European companies has earned us the trust of businesses like retailers, manufacturers, and financial services providers.
>
> Please visit our Compliance Resource Center for a complete listing of our compliance offerings..

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 concerns about cybersecurity have led to governments and organisations working together to shape cybersecurity requirements and frameworks, including:

- Global Standards, such as ISO 27001 and ISO 27017, and the Cloud Controls Matrix from the Cloud Security Alliance
- EU regulations such as the EUCA and the ENISA Security Guidelines under the EECC
- National frameworks such as BSI C5 in Germany, ENS in Spain or PiTuKri in Finland.

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, summarised in this security overview whitepaper. Other whitepapers detail our security practices in specific areas, such as encryption at rest, encryption in transit, and infrastructure security. Google Cloud also publishes guidance on security best practices, use cases, and blueprints.
>
> Google Cloud’s security, third-party audits, and certifications help support your

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. Some of the key international and national standards we are audited against include:

- ISO 27001 (Information Security Management)
- ISO 27017 (Cloud Security)
- CSA Star Cloud Controls Matrix
- BSI C5:2020 (Germany)
- ENS (Spain)
- PiTuKri (Finland).

Data privacy and communications confidentiality

CSPs are entrusted with large volumes of sensitive customer data, including personally identifiable information and communications records for entire societies. Therefore, the consequences of any data breaches are very serious. Such personal data is protected in Europe under GDPR, with potentially substantial fines for non-compliance.

European and national law (including the European Convention on Human Rights and ePrivacy) also recognises the confidentiality of communications as a fundamental right. This right protects individuals from unauthorised interception and surveillance of their private communications.

Protecting customer data privacy and confidentiality of communications are fundamental requirements for telecom operators. In the European context, this means ensuring compliance with GDPR and ePrivacy.

How we help: Google Cloud's trust principles provide a starting point for our approach to data privacy. Our commitment to European customers includes the following:

- Our compliance with GDPR
- Our support for the Enhanced SCCs
- The support we offer to customers carrying out a Data Processing Impact Assessment (DPIA)

As a member of EU Cloud CoC, Google Cloud has been assessed by SCOPE Europe at the second level of compliance, which demonstrates a commitment to implementing data protection and security policies that align with the GDPR.

We also support the supplementary measures recommended by the European Data Protection Board. For more information, refer to our whitepapers on trusting your data with Google Cloud and safeguards for international data transfers.

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

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

Further information is available from Google Cloud's Privacy Resource Center.

Data residency

When moving to a cloud environment, CSPs face the challenge of validating, then controlling where their data resides. In a European context, this means controlling the location of customer data and limiting any potential transfers of this data to non-compliant locations. In many cases, retaining such sensitive data within the EU is sufficient. However, there are some cases where certain data categories are required to remain within a specific country.

How we help: The majority of Google's Public Cloud services can be configured for data residency to control the physical location of customer data. Google Cloud has regions in ten European countries (UK, France, Germany, Spain, Italy, Switzerland, Netherlands, Belgium, Poland and Finland), with four more regions announced (Norway, Sweden, Austria and Greece) - providing customers with many options for data localisation.

Remote access to data (for reasons such as technical support) can be considered a data transfer. To help customers address this concern, Google Cloud administrator access to customer data can be limited via Access Approval and monitored via Access Transparency. For EU-based customers, Google Cloud offers additional data residency support (including EU-based technical support) via Assured Workloads.

For more details, refer to this whitepaper on data residency and operational transparency for European customers.

Operational requirements

Should the availability of public communication services be impacted by a security incident, a widespread disruption could occur, including the possible inability to contact emergency services, and the consequences could be measured in human lives lost. CSPs could also face fines, reputational damage, and loss of business.

European regulations (such as the European Electronic Communications Code) require CSPs to take appropriate measures to safeguard the availability and integrity of their services. This means ensuring continuous operations and service availability, even in unexpected circumstances. CSPs must design for high availability and plan for business continuity and disaster recovery. CSPs also require oversight of software changes that could impact their services to ensure that software deliverables do not compromise service availability or introduce security vulnerabilities.

How we help: CSPs are responsible for ensuring they are designing for high availability (as well as security) when planning cloud solutions. Google Cloud publishes architecture guidelines to assist with this. 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 own 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 also offers a number of 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 to carry 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), utilising 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 provides a bundle of 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 CSP infrastructure and systems, and CSPs are increasingly adopting APIs that expose their capabilities.

The WAAP solution includes the following products:

- Cloud Armor
- reCAPTCHA Enterprise
- Apigee API Management

Risk and Compliance as Code (RCaC) solution

Achieving, maintaining, and demonstrating compliance with relevant security regulations is critical for all CSPs. Google Cloud's Risk and Compliance as Code (RCaC) solution combines several capabilities to help meet this challenge.

By adopting this solution, CSPs can prevent non-compliance by asserting infrastructure and policies as code for easy onboarding to Google Cloud and establish secure guardrails from the get-go via security blueprints and Assured Workloads. Additionally, they can detect non-compliance via Security Command Center, notify stakeholders when offending infrastructure is identified, and reduce risk with intelligent automation, control mapping, and continuous assessments. Finally, once on Google Cloud, CSPs can leverage Risk Manager to continuously evaluate risk and utilise our Risk Protection Program to qualify for cyber insurance.

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 CSPs 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.

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

For more information, refer to our Autonomic Security Operations whitepaper.

Software Delivery Shield solution

Google Cloud's Software Delivery Shield offers a fully managed, end-to-end solution that enhances software supply chain security across the entire software development life cycle from development, supply, and CI/CD to runtimes.

As CSPs move towards software-based networks and adopt cloud-native applications and modern software development processes (including automated testing, deployment, and faster and more numerous deployments), new security challenges emerge. A modern software development and deployment pipeline with secure and automated DevOps processes has become more critical than ever.

Using this solution, CSPs can:

- Enhance application security in development environments
- Improve the security of application images and dependencies
- Strengthen the security of CI/CD pipelines
- Protect running applications
- Enforce trust-based security policies throughout SDLC.

Conclusion

CSPs across Europe are looking to transform and grow their business. Digital transformation initiatives include modernising of 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 monetise their data by adopting cloud-based analytics and ML to gain insights from their customer and network data.

Google Cloud is helping CSPs transition to the cloud while keeping in step with applicable laws, regulations, and guidance. Google Cloud continues to innovate in areas such as encryption, key management, auditability and transparency, data residency, and localised support to help CSPs meet their operational security, resilience, and data privacy needs.

Google Cloud is committed to keeping in step with telecom laws and regulations, to meet the evolving needs of CSPs and consumer demand in the telecommunications industry.

Appendix - Security standards, regulations, and guidelines

This appendix contains a survey of relevant global, regional, and national security standards, regulations, and guidelines for European 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 (and are not regulations backed by law) but are widely accepted as a baseline for good security practices and provide a way to measure organisational compliance to internationally recognized security policies:

- 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)
- CSA SOC2+ demonstrates compliance with the Cloud Security Alliance Cloud Controls Matrix (CCM) - designed to help customers assess and select a Cloud Service Provider.

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

European Union Regulation

European institutions and legal frameworks

The European Union (EU) is a united charter of 27 European countries referred to as member states. The EU has certain powers granted by the member states including the ability to pass directives and create regulatory frameworks (collectively, EU legal codes).

Several non-EU member states share agreements and cooperate closely with the EU. Norway, Iceland, and Liechtenstein are members of the European Economic Area (EEA) and European Free Trade Association (EFTA) and respect the “four freedoms”[2]. Switzerland is not a member of the EEA but is a member of the EFTA and has bilateral agreements with the EU. All four nations have aligned on some EU legal codes (such as GDPR).

[2] Free movement of goods, services, persons, and capital

The United Kingdom (UK) is a former member of the EU and retains many former EU legal codes within its national legislation (such as GDPR). The UK also continues to adopt some new EU legal codes (such as the EECC). The UK is not a member of either the EEA or the EFTA.

The remaining European countries (Albania, Andorra, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, San Marino, Serbia and Ukraine) maintain independent legal systems. They are not members of either the EEA or EFTA.

General Data Protection Regulation (GDPR)

On April 27, 2016, the EU Parliament passed "Regulation (EU) 2016/679", establishing the GDPR regulatory framework.

The main objective of GDPR is the **protection of consumer rights and personal data** for EU citizens. However, the ubiquitous nature of international corporations and communications means the effects of GDPR are felt outside of the EU. Many countries worldwide also adapt or assimilate parts of GDPR for their data privacy regulations.

Google Cloud commits in our contracts to comply with the GDPR in relation to our processing of customer personal data in all Google Cloud services.

EU Standard Contractual Clauses (SCC)

Under GDPR, transfers of personal data outside of the EU and EEA are not permitted unless adequate safeguards are used.

One possible safeguard is an EU Commission adequacy decision (that the destination country's data protection laws are essentially as good as GDPR). An alternative safeguard is Standard Contractual Clauses (SCCs), designed to impose various **contractual obligations to safeguard the personal data** of EU citizens transferred outside of the EEA. On June 4, 2021, the EU Parliament updated the original SCCs passed in 2010 to align with GDPR data protection and cybersecurity requirements.

The European Data Protection Board (EDPB) has also published recommendations on the "supplementary measures" that can be used in conjunction with the SCCs to protect data that may be transferred outside of the EU. Review our whitepaper on the Safeguards for international data transfers with Google Cloud for more information.

Google Cloud has adopted the updated SCCs.

EU Cloud Code of Conduct (CoC)

The EU Cloud CoC was published by the cloud community with the cooperation of the EU Parliament. With approval by the Belgian Data Protection Authority in May 2021, the EU Cloud CoC has become a sufficient guarantee pursuant to Article 28.5 of GDPR for Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). Cloud providers can demonstrate sufficient data protection and cybersecurity requirements to cloud customers by voluntarily becoming members of and testing against the EU Cloud CoC.

Google Cloud has demonstrated adherence to the EU Code Of Conduct, at the second level of compliance.

ePrivacy Regulation (ePR)

The ePrivacy Directive (“**Directive 2002/58/EC**”) came into force in July 2002. This directive protects the confidentiality of both communications content (e.g. telephone calls or text messages) and communications metadata (e.g. called and calling parties, locations, time, and duration of communication).

The ePrivacy Regulation (ePR), will replace the ePrivacy Directive, which is currently being drafted.

European Electronics Communication Code (EECC)

On December 11, 2018, EU Parliament passed the “Directive 2018/1972”, establishing the European Electronics Communication Code, which reforms the EU telecommunications regulatory framework and replaces previous EU legislation, including the 2009 Framework Directive for Telecommunications. The objectives of the EECC include boosting telecoms’ connectivity and performance while increasing protection for consumers. Article 40 of the EECC requires operators "take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services". Specific details are delegated to ENISA. From October 2024, it is expected that Article 40 of the EECC will cease to apply and will be replaced by NIS2 (see below).

ENISA security guidelines under the EECC

ENISA (the EU Agency for Cybersecurity) has published Guidelines on Security Measures under the EECC to meet the **security and risk requirements** of **Articles 40/41 of the EECC**. This document is non-binding at the EU level, but member states may choose to make the requirements binding at the national level. The guidelines are broken down by objectives and sophistication to help CSP organisations select security measures that are appropriate and proportional to the risk.

The measures in this guideline can be mapped to ISO 27001/27002 (or, in the case of Cloud, to ISO 27001/27017). Google Cloud is certified as compliant with ISO/IEC 27001 and ISO/IEC 27017.

ENISA has also published a 5G Cybersecurity Toolbox, which offers security recommendations to EU member states regarding the supply, deployment, and operation of 5G Network Equipment.

The EU Cybersecurity Act

The EU Cybersecurity Act (EUCA) of 2019 created a permanent mandate for ENISA and introduced a uniform European **cybersecurity certification framework** for ICT products, services and processes.

As part of the effort to ensure the security of networks across Europe, ENISA has worked with the NIS Cooperation Group and European Council to develop guidelines for a common level of cybersecurity throughout the EU. These efforts include the "NIS2 Directive", which aims to "strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements".

Google Cloud has published a blog regarding NIS2 and our support for the European Cybersecurity ecosystem.

EU Cloud Switching Cloud Providers and Porting Data (SWIPO)

SWIPO is a group of non-governmental stakeholders (such as Google and Microsoft) facilitated by the EU Parliament to support Article 6 of the Free Flow of Non-Personal Data Regulation. SWIPO has created voluntary Codes of Conduct, one each for SaaS and IaaS. The Codes' main objective is to facilitate the migration of customer data from one CSP to another. Once a member joins SWIPO, they are governed by the Codes to ensure a trusted relationship with cloud customers.

As a stakeholder, we are fully committed to the Codes laid out by SWIPO and provide all the tools necessary for our customers to view, delete, download, and transfer their content.

National regulation (EU member states)

EU member states are required to adopt EU directives by transposing them into national legislation within the deadline set by the individual directive. The standard transposition period is two years.

Information on country-level regulation for selected EU member states is described below. They are organised alphabetically by country.

Finland: Regulation on Information Security in Telecommunications Operations Networks

The Republic of Finland enacted the latest version of the telecom regulatory framework with the passage of the "**Act 917/2014 on Electronic Communications Services**" on November 7, 2014[3]. Within the act, "**Chapter 29**" gives the Finnish Transport and Communications Agency (Traficom) regulatory authority to ensure cybersecurity and data protection within the telecom sector.

As part of their responsibility, Traficom enacted the regulation "**FICORA 67 A/2015 M**" (Regulation on Information Security in Telecommunications Operations Networks), which offers guidance and instructions to maintain the principle of confidentiality, integrity, and availability[4].

[3] Act on Electronic Communications Services, Republic of Finland

[4] FICORA 67 A/2015 M, Republic of Finland

France: Code des Postes et des Communications Électroniques (Code on Posts and Electronic Communications, CPCE)

The French Republic established the **CPCE** as the regulatory framework for telecommunications, and Autorité de Régulation des Communications Électroniques, des Postes et de la Distribution de la Presse (ARCEP, Electronic Communications, Postal, and Print Media Distribution Regulatory Authority) is the regulatory authority for the enforcement of the CPCE. The CPCE is a catch-all framework for laws and regulations that French telecoms must comply with and has been amended multiple times. A recent example is the "**Ordinance n° 2021-650 of May 26, 2021**", which transposed EECC into law[5].

Germany: BSI Cloud Computing Compliance Criteria Catalog (C5:2020)

BSI C5:2020 is a German government program that enables the adoption of cloud products and services while emphasising the need to maintain stringent security controls over federal information. To provide products and services to government agencies, a telecom provider needs to be C5:2020 authorised in accordance with the Federal Office for Information Security (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, BSI). Telecom entities are assessed against industry-recognised security standards (such as ISO/IEC 27001, Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) and American Institute of Certified Public Accountants (AICPA) Trust Services Principles (TSP))[6].

Google Cloud has achieved an attestation against the C5:2020 requirements.

Germany: Bundesdatenschutzgesetz (Federal Data Protection Act, BDSG)

Germany originally published data protection and cybersecurity guidelines for companies processing, storing, or transmitting personal data of German citizens on June 30, 2017, with the "**Federal Law Gazette I p. 2097**", establishing the BDSG. On June 23, 2021, BDSG was updated to transpose GDPR regulatory framework requirements[7].

Germany: Telekommunikation Modernisierungsgesetz (Telecommunications Modernization Act, TKMoG)

Germany originally published telecommunication and technology regulations on July 25, 1996, with the "**Federal Law Gazette I p. 1190**" establishing the Telecommunications Act (Telekommunikationsgesetz, TKG). On June 23, 2021, TKG was amended with the TKMoG to transpose EECC and bring the regulatory framework in line with new and emerging industry trends[8].

[5] French Telecommunication Regulations, DLA Piper

[6] Cloud Computing Compliance Controls Catalogue, Federal Republic of Germany,

[7] Federal Data Protection Act, Federal Republic of Germany

[8] Telecommunications Act, Federal Republic of Germany

Germany: Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (Information Technology Security Act 2.0)

On April 23, 2021, Germany enacted the **Information Technology Security Act 2.0** to transpose the EU Cybersecurity Act into federal law. The objectives of the Information Technology Security Act 2.0 include:

- **Detection and defence**
- **Cybersecurity in mobile networks**
- **Consumer protection**
- **Security for business**
- Naming BSI the National Cybersecurity Certification Authority[9]

Italy: Electronic Communications Code

The Italian Republic enacted the original "**D.lgs. No. 259/2003**" (Electronic Communications Code) on September 16, 2003[10]. The Electronic Communications Code was amended on December 24, 2021, with the "**D.lgs. No. 207/2021**", which transposes the EECC into national law. The updated legislation also includes further enhancements related to data privacy, including updating the internet as a means of communication, improving consumer transparency for electronic communications, and more[11].

Italy: National Cybersecurity Agency

The Italian Republic formally approved "**Decree No. 82 of 14 June 2021**" to establish urgent provisions on cybersecurity and define the national cybersecurity architecture. The decree was officially enacted into law with the amendment "**Law 4 August 2021, n. 109**" to establish the National Cybersecurity Agency (including CSIRT Italia). The National Cybersecurity Agency is currently adopting and assisting in the drafting of regulatory acts (such as the **Italian Cloud Strategy**)[12].

Poland: Telecommunications Act

On July 16, 2004, the Republic of Poland enacted the **Telecommunications Act**[13]. The act has seen multiple amendments, including the latest in 2013. The act and subsequent amendments have prioritised competition, growth, and **infrastructure security objectives**[14].

Spain: General de Telecomunicaciones (General Telecommunications Law)

The Kingdom of Spain enacted the original "**Law No. 9/2014**" (General Telecommunications Law) on May 9, 2014, establishing a framework to regulate telecom operators. With the "**Law No. 11/2022**" established on June 28, 2022, the General Telecommunications Law has been

[9] Second act on increasing the security of IT systems (German IT Security Act 2.0), Federal Republic of Germany

[10] Electronic Communications Code, Italian Republic

[11] Transposition of the European Electronic Communications Code, Italian Republic

[12] National Cybersecurity Agency, Italian Republic

[13] Telecommunications Act, Republic of Poland

[14] Telecoms, Media and Internet in Poland, Republic of Poland

updated to transpose EECC. Specifically, “**Article 60**” establishes cybersecurity requirements for telecom operators.

Additionally, data privacy as related to GDPR and ePR is strengthened with “**Article 66(1)(a)**”, which specifies that consumers will not receive automated or unwanted communications (e.g., calls, faxes,) without prior consent or unless the communication is covered under a legal basis. According to “**Article 66(1)(b)**”, the data privacy aspects of the law will not come into force until June 23, 2023[15].

Spain: Esquema Nacional de Seguridad (National Security Framework, ENS)

Spain originally published data protection and cybersecurity guidelines for companies processing, storing, or transmitting personal data of Spanish citizens on January 8, 2010, with the “**Royal Decree 3/2010**”, establishing the ENSNational Security Framework (ENS). A regular security status report is published as required by “**Article 35**”. In response to the evolution of technology, cyber threats, and the EU landscape revealed through these reports, ENS was amended by the “**Royal Decree 951/2015**” on November 4, 2015[16].

Google Cloud has met the requirements to comply with ENS at the “High” level.

Spain: Security of 5G Electronic Communications Networks and Services

On March 30, 2022, Spain enacted the “**Law 7/2022**” to transpose the EUCA into their national legislation. The legislation intends to bring cybersecurity frameworks and regulations to new and growing technologies (such as 5G) and foster the growth of telecoms[17].

Sweden: Dataskyddsförordningen (GDPR)

In 2018, the Kingdom of Sweden adopted GDPR with no changes. The Swedish Authority for Privacy Protection (Integritetsskydds Myndigheten, IMY) has published various articles on what GDPR means and how to file complaints[18].

National regulation (Non-EU member states)

Non-EU member states are not obliged to adopt EU laws. However, as discussed above, some non-EU countries choose to adopt some EU directives (such as GDPR) to facilitate economic cooperation (including data transfers) with EU member states.

Norway: Electronic Communications Act

The Kingdom of Norway enacted the original “**ACT-2003-07-04-83**” (Electronic Communications Act) on July 25, 2003. The “**LOV-2021-06-18-131**” is the latest amendment to the act, which came into force on January 1, 2022. The amendments to the Electronic Communications Act added or strengthened requirements for cybersecurity and

[15] General Telecommunications Law, Kingdom of Spain

[16] National Security Scheme, ENS, Kingdom of Spain,

[17] Security of 5G Electronic Communications Networks and Services, Kingdom of Spain,

[18] Data Protection, Swedish Authority for Privacy Protection

communications privacy. Specifically, the section "**§ 2-7. Protection of Communications and Data**" addresses the security measures telecom operators should take, and the section "**§ 2-7 b. Use of Cookies**" addresses cookie consent requirements[19].

Norway: Regulations on Electronic Communications Networks and Services (eCommunications Regulations)

On July 22, 2004, Norway enacted the "**FOR-2004-02-16-401**" (eCommunications Regulations). The regulations have been amended multiple times since entry into force, with some provisions being added or repealed. The latest amendment was the "**FOR-2022-12-22-2491**" on January 1, 2023. The eCommunications Regulations contain objectives for data privacy and cybersecurity, especially within "**Chapter 7. Protection of Communications**", "**Chapter 8. Security and Preparedness**", and "**Chapter 9. Private Electronic Communication Networks**".

The regulations contain specific provisions for processing personal data and communications (including obtaining consent), maintaining the confidentiality of personal data, maintaining the security of networks, and more[20].

Norway: Personal Data Act

Norway officially enacted the "**LOV-2018-06-15-38**" regulation to transpose the GDPR regulatory framework into the Personal Data Act on July 6, 2018[21].

Norway: National Security Act and National Security Strategy

On January 1, 2019, Norway enacted the "**LOV-2018-06-01-24**" (National Security Act) to ensure the protection of national security interests (such as **critical infrastructure**). The National Security Act contains objectives on data privacy and cybersecurity. Specifically, the government cannot view or process personal data beyond what is necessary to achieve a defined purpose, and digital infrastructure should be protected from cyber-attacks (including response and warning systems)[22].

To facilitate an overall national cybersecurity strategy, public and private stakeholders have regularly published a strategy whitepaper since 2003. On January 1, 2019, Norway published the latest "**National Cyber Security Strategy for Norway**" to address both public and private cybersecurity issues due to the rapid pace of digitalisation. The government and stakeholders in critical infrastructure, including telecom operators, cooperated to define **cybersecurity challenges** and the **strategies** to address them[23].

Switzerland: Revised Federal Data Protection Act (revFDPA)

The Federal Assembly of the Swiss Confederation passed the original Federal Data Protection

[19] Electronic Communications Act, Kingdom of Norway

[20] Regulations on Electronic Communications Networks and Services, Kingdom of Norway

[21] Personal Data Act, Kingdom of Norway

[22] National Security Act, Kingdom of Norway

[23] National Security Strategy for Norway, Kingdom of Norway

Act (FDPA) on June 19, 1992. It transposed the EU data protection regulatory framework from GDPR into law on March 1, 2019. revFDPA brings Switzerland's telecommunications regulatory framework in line with EU data protection and cybersecurity requirement expectations[24].

Google Cloud is committed to revFPDA compliance for Google Cloud services where applicable.

UK Communications Act 2003

On July 17, 2003, the UK enacted the Communications Act to create a regulatory framework for the telecom sector. The Communications Act contains objectives for customer protection (such as privacy and transparency) and cybersecurity e.g., protecting critical infrastructure, preventing unauthorised access).

The Communications Act has seen multiple amendments since it entered into force, including the Electronic Communications and Wireless Telegraphy Regulations 2020, which transposed the EECC. Note that the UK withdrew from the European Union in 2019, but the UK Government adopted the EECC to maintain alignment with European telecoms regulations.

UK Data Protection Act 2018 (DPA)

On May 23, 2018, the United Kingdom (UK) passed the "**2018 Chapter 12**" (DPA), which transposed the EU data protection regulatory framework GDPR into law for any company which processes, stores, or transmits personal data of UK citizens. The objectives of the Data Protection Act include data protection and cybersecurity (e.g., data residency, encryption of data at rest or in transit, lawful use, transparency).

UK Telecommunication (Security) Act 2021 (TSA)

The Telecommunications (Security) Act 2021 (TSA) introduces new duties to providers of public electronic communications networks. These duties aim to identify and reduce the risk of security compromises, and place regulations on providers to prevent and mitigate any adverse effects of security compromises.

The security measures imposed by the TSA are further detailed by the Electronic Communications (Security Measures) Regulations 2022 and the Telecoms Security Code Of Practice.

UK National Cyber Security Centre (NCSC)

The UK National Cyber Security Centre (NCSC) aims to make the UK a safe place for online business. The NCSC aims to protect UK citizens from cyber-attacks by managing major incidents and improving underlying security through technological improvements.

[24] Federal Act on Data Protection, Swiss Confederation

Cloud Security

The NCSC publishes Cloud Security Guidance, including 14 Cloud Security Principles, to help UK organisations choose a cloud provider that meets their security needs. This guidance is not specific to telecoms but may interest CSPs.

Google Cloud is compliant with the NCSC Cloud Security Principles.

Cyber Essentials Plus

Cyber Essentials is a government scheme to help protect organisations from cyber-attacks. There are two levels of certification - Cyber Essentials and Cyber Essentials Plus. Cyber Essentials is a self-assessment to evaluate an organisation's vulnerability against cyber-attacks. Organisations can self-assess against five controls that cover the basics of adequate information security, including firewalls, secure configuration, access controls, malware, and patch management. Cyber Essentials Plus is similar to Cyber Essentials but requires a technician to verify against the same controls to be certified.

Google Cloud provides information on how our products and services align with these Cloud Security Principles.