Government Regulation No. 71

GCP and Google Workspace Mapping

This document is designed to help customers regulated by Indonesia Government Regulation No. 71 ("GR 71") to consider GR 71 in the context of Google Cloud Platform ("**GCP**") and Google Workspace.

We focus on requirements applicable to Electronic System Providers, as defined in Article 1(4)-(6) and Article 2 of GR 71, but it does not contain the entirety of GR 71. For each Article, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and controls.

#	GR 71	Google Cloud Commentary
1.	*Division 1 "General", Article 3* (1) Any Electronic System Provider shall organize Electronic System in a reliable and safe manner as well as be responsible for the proper operation of the Electronic System. (2) The Electronic System Provider shall be responsible for the organization of its Electronic Systems. (3) The provisions as referred to in paragraph (2) do not apply in the event that the occurrence of force majeure, fault, and/or negligence of the Electronic System User may be proven.	This is a customer consideration.
2.	*Division 1 "General", Article 4* Insofar that it is not stated otherwise by separate laws and regulations, any Electronic System Provider must operate Electronic System which fulfills the minimum requirements as follows: a. able to redisplay Electronic Information and/or Electronic Document as a whole in accordance with the retention period which is determined with laws and regulations; b. able to protect the availability, integrity, authenticity, privacy, and accessibility of Electronic Information in the organization of such Electronic System; c. able to operate in accordance with the procedures or guidelines in the organization of such Electronic System; d. is equipped with procedures or guidelines which are announced with a language, information, or symbol which may be understood by the relevant party with the organization of such Electronic System; and e. has a sustainable mechanism to maintain novelty, clarity and accountability of the procedures and guidelines.	The confidentiality and integrity of a cloud service consists of two key elements: Security of Google's infrastructure Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Given the one-to-many nature of our service, Google provides the same robust security for all our customers. Google provides detailed information to customers about our security practices so that customers can understand them and consider them as part of their own risk analysis. More information is available at: ● Our infrastructure security page ● Our security whitepaper ● Our cloud-native security whitepaper ● Our infrastructure security design overview page ● Our security resources page Google recognizes that customers expect independent verification of our security, privacy and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance.

Government Regulation No. 71

GCP and Google Workspace Mapping

		Google commits to comply with the following key international standards during the term of our contract with you: • ISO/IEC 27001:2013 (Information Security Management Systems) • ISO/IEC 27017:2015 (Cloud Security) • ISO/IEC 27018:2014 (Cloud Privacy) • PCI DSS • SOC 1 • SOC 2 • SOC 3 Security of your data and applications in the cloud Customers define the security of their data and applications in the cloud. This refers to the security measures that customers choose to implement and operate when they use the Services. (a) Security by default Although we want to offer customers as much choice as possible when it comes to their data, the security of their data is of paramount importance to Google and we take the following proactive steps to assist them: • **Encryption at rest.** Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available at: https://cloud.google.com/security/encryption-at-rest/default-encryption. • **Encryption in transit.** Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. More information is available at https://cloud.google.com/security/encryption-in-transit. (b) Security products In addition to the other tools and practices available to customers outside Google, customers can choose to use tools provided by Google to enhance and monitor the security of their data. Information on Google's security products is available on our Cloud Security Products page. (c) Security resources Google also publishes guidance on:

Government Regulation No. 71

GCP and Google Workspace Mapping

		3. Security best practices 4. Security use cases
3.	*Division 1 "General", Article 5* (1) The Electronic System Provider must ensure that their Electronic System does not contain Electronic Information and/or Electronic Document which are prohibited in accordance with laws and regulations. (2) The Electronic System Provider must ensure their Electronic System does not facilitate the dissemination of prohibited Electronic Information and/or Electronic Document in accordance with laws and regulations. (3) The provision on the obligation of the Electronic System Provider as referred to in paragraph (1) and paragraph (2) shall be regulated with Regulation of the Minister.	Given the nature of the services, Google does not control the data used by customers.
4.	*Division 3 "Hardware," Article 7* (1) Hardware which is used by the Electronic System Provider shall: a. meet the security, interconnectivity and compatibility aspects with the used system; b. have technical support services, maintenance services, and/or aftersales services from the seller or the provider; and c. have a service continuity warranty. (2) The fulfillment of requirements as referred to in paragraph (1) shall be conducted through certification or other similar evidences.	Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Refer to Row 2 for more information and Appendix 2 (Security Measures) of the DPA and DPST.
5.	*Division 4 "Software," Article 8* The Software which is utilized by the Electronic System Provider shall: a. be guaranteed of the security and reliability of proper operation; and b. ensure of the continuity of the services	Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services. Refer to Row 2 for more information and Appendix 2 (Security Measures) of the DPA and DPST.
6.	*Division 4 "Software," Article 9* (1) The developer who provides Software which is specifically developed for the Electronic System Provider in the Public Sector must submit the source code and documentation of the Software to the relevant Agency or institution. (2) The relevant Agency or institution as referred to in paragraph (1) must retain the source code and documentation of the Software in a facility in accordance with laws and regulations.	This is a customer consideration.

Government Regulation No. 71

GCP and Google Workspace Mapping

	(3) In the event that the facility as referred to in paragraph (2) is not yet available, the Agency or institution may retain the source code and documentation of the Software to a trusted third party which retains the source code. (4) The developer must guarantee the acquisition and/or Access to the source code and documentation of the Software to the trusted third party as referred to in paragraph (3). (5) The Electronic System Provider in the Public Sector must guarantee the confidentiality of the utilized Software source code and is only utilized for the benefit of the Electronic System Provider in the Public Sector. (6) Further provisions on the obligation to transfer the source code and documentation of the Software to the Agency or institution as referred to in paragraph (1) and the retention of source code and documentation of the Software to a trusted third party as referred to in paragraph (3) shall be regulated with Regulation of the Minister.	
7.	*Division 6 "Electronic System Governance", Article 11* (1) The Electronic System Provider shall guarantee: a. the availability of service level agreement; b. the availability of information security agreement on the utilized Information Technology services; and c. the security of the organized information and internal communication facilities. (2) The Electronic System Provider as referred to in paragraph (1) shall ensure that any component and integrity of all Electronic System operates properly.	This is a customer consideration. The SLAs contain Google's commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page (for GCP) and on the Google Workspace Service Level Agreement page (for Google Workspace)
8.	*Division 6 "Electronic System Governance", Article 14* (1) The Electronic System Provider must implement the principles of Personal Data protection in processing Personal Data consisting of: a. Personal Data collection is conducted in a limited and specific manner, legally valid, fair, with consent and agreement of the Personal Data owner; b. Personal Data processing is conducted in accordance with its intention; c. Personal Data processing is conducted by ensuring the rights of the Personal Data owner; d. Personal Data processing is conducted accurately, completely, not misleading, up-to-date, accountable, and taking the intention of Personal Data processing into consideration; e. Personal Data processing is conducted by protecting the Personal Data security from loss, misappropriation, Access and illegal disclosure, as well as alteration or destruction of Personal Data;	This is a customer consideration. Google will comply with the customer's instructions for the processing of data. Google also provides functionality to enable customers to access, rectify, and restrict processing of their data as well as retrieve or delete data. See Section 5 (Processing of Data) of the DPA and DPST. See also Section 9 (Access etc.; Data Subject Rights; Data Export) of the DPA and DPST.

	f. Personal Data processing is conducted by notifying the purpose of collection, processing activities, and failure in protecting Personal Data; and g. Personal Data processing is destroyed and/or deleted unless in a retention period in accordance with the need based on laws and regulations. (2) Personal Data processing as referred to in paragraph (1) shall consist of: a. acquisition and collection; b. processing and analysis; c. retention; d. improvement and update; e. display, announcement, transfer, dissemination, or disclosure; and/or f. deletion or destruction. (3) Personal Data processing shall comply with the provisions of a valid agreement from the Personal Data owner for 1 (one) or certain purposes which have been delivered to the Personal Data owner. (4) Other than the approval as referred to in paragraph (3), the Personal Data processing shall fulfill the provisions which are required for: a. the fulfillment of contractual obligation in the event that the Personal Data owner is one of the parties or to fulfill the request of the Personal Data owner upon entering into an agreement; b. fulfillment of legal obligation from the Personal Data controller in accordance with laws and regulations; c. fulfillment of vital interest of the Personal Data owner; d. implementation of Personal Data controller authority based on laws and regulations; e. fulfillment of Personal Data controller obligation in public services for the public interest; and/or f. fulfillment of other vital interests of the Personal Data controller and/or Personal Data owner. (5) If there is a failure in protecting the managed Personal Data, the Electronic System Provider must notify in writing to the Personal Data owner. (6) Provisions on technical processing of Personal Data are regulated with laws and regulations.	
9.	*Division 6 "Electronic System Governance", Article 15* (1) Any Electronic System Provider must delete irrelevant Electronic Information and/or Electronic Document which are under their control based on the request of the relevant person. (2) The obligation to delete irrelevant Electronic Information and/or Electronic Document as referred to in paragraph (1) shall consist of: a. erasure (right to erasure); and b. delisting from search engine (right to delisting).	This is a customer consideration. Google provides functionality to enable customers to access, rectify, and restrict processing of their data as well as retrieve or delete data. See Section 6 (Data Deletion) of the DPA and DPST. See also Section 9 (Access etc.; Data Subject Rights; Data Export) of the DPA and DPST.

	(3) The Electronic System Provider which must delete Electronic Information and/or Electronic Document as referred to in paragraph (1) is the Electronic System Provider which obtains and/or process Personal Data under their control.	
10.	*Division 6 "Electronic System Governance", Article 18* (1) Any Electronic System Provider must provide a mechanism to delete the irrelevant Electronic Information and/or Electronic Document in accordance with laws and regulations. (2) The deletion mechanism as referred to in paragraph (1) shall at least contain provisions on: a. provision of a communication channel between the Electronic System Provider with the Personal Data owner; b. feature to delete irrelevant Electronic Information and/or Electronic Document which enables the Personal Data owner to delete their Personal Data; and c. recordation for the request to delete irrelevant Electronic Information and/or Electronic Document. (3) Further provisions on the deletion mechanism as referred to in paragraph (1) and paragraph (2) shall be regulated with Regulation of the Minister. (4) Provisions on the deletion mechanism in certain sectors may be established by the Ministry or relevant Body after coordinating with the Minister	Refer to Row 9.
11.	*Division 6 "Electronic System Governance", Article 19* (1) The Electronic System Provider shall implement good and accountable governance for the Electronic System. (2) The governance as referred to in paragraph (1) shall at least fulfill the following requirements: a. the availability of procedures and guidelines in the organization of Electronic System which is documented and/or announced with a language, information, or symbol which is understood by the party who is in relation to the organization of such Electronic System; b. there is a sustainable mechanism to maintain novelty and clarity of the implementing guidelines procedures; c. there is an institutional and completeness of supporting personnel for the proper operation of Electronic System; d. there is an implementation of performance management in the Electronic System which is organized to ensure that the Electronic system operates properly; and e. there is a plan to maintain the continuity of the organization of the managed Electronic System.	This is a customer consideration. Google provides documentation to explain how institutions and their employees can use our GCP services, as well as documentation for our Google Workspace services. If an institution would like more guided training, Google also provides a variety of courses and certifications.

Government Regulation No. 71

GCP and Google Workspace Mapping

	(3) Other than requirements as referred to in paragraph (2), the relevant Ministry or Body may determine other requirements which are established in laws and regulations.	
12.	*Division 6 "Electronic System Governance", Article 20* (1) The Electronic System Provider in the Public Sector must own a business continuity plan to overcome disturbance or disaster in accordance with the risk of the impact it causes. (2) The Electronic System Provider in the Public Sector must conduct management, processing, and/or retention of the Electronic System and Data Electronic in Indonesian territory. (3) The Electronic System Provider in the Public Sector may conduct management, processing, and/or retention of the Electronic System and Electronic Data outside of the Indonesian territory in the event that the retention technology is not available domestically. (4) The retention technology criteria is not available domestically as referred to in paragraph (3) shall be determined by a committee consisting of the ministry who is in charge of governmental affairs in the communication and informatics sector, body who is in charge of affairs in technology review and implementation, body who is in charge of affairs in cybersecurity, and the relevant Ministry or Body. (5) The establishment of the committee as referred to in paragraph (4) is determined by the Minister. (6) In the event that the Electronic System Provider in the Public Sector utilizes third-party services, the Electronic System Provider in the Public Sector must conduct data classification in accordance with the inflicted risk. (7) Further provisions on data classification in accordance with risk as referred to in paragraph (6) shall be regulated with Regulation of the Minister.	This is a customer consideration. Google recognizes the importance of business continuity and contingency planning. We do our own planning for our services. Customers can also use our services in their own business continuity and contingency planning. Information about how customers can use our GCP services in their own disaster recovery and business contingency planning is available in our Disaster Recovery Planning Guide. Information on the reliability of our Google Workspace services is available on our Google Cloud Help page. Google provides you with choices about where to store your data. Once you choose where to store your data, Google will store your data at rest only in the selected region(s) and in accordance with our Service Specific Terms and Terms of Service. You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper and our Trusting your data with Google Workspace whitepaper.
13.	*Division 6 "Electronic System Governance", Article 21* (1) The Electronic System Provider in the Private Sector may conduct management, processing, and/or retention of the Electronic System and Electronic Data in Indonesian territory and/or outside of Indonesian territory. (2) In the event that the Electronic System and Electronic Data are managed, processed, and/or retained outside of Indonesian territory, the Electronic System Provider in the Private Sector must ensure the effectiveness of supervision by the Ministry or Body and law enforcement. (3) Electronic System Provider in the Private Sector must provide Access to the Electronic System and Electronic Data for the purpose of supervision and law enforcement in accordance with laws and regulations.	Google recognizes that using our services should not impair the competent authority's ability to supervise compliance with applicable laws and regulations. Google grants information, audit and access rights to customers and their appointees. See Section 7.5.2 (Customer's Audit Rights) of the DPA and DPST.

Government Regulation No. 71

GCP and Google Workspace Mapping

	(4) Provisions on management, processing, and retention of Electronic System and Electronic Data for the Electronic System Provider in the Private Sector in the financial sector shall be further regulated by the regulatory and supervisory authority in the financial sector.	
14.	*Division 7 "Security of Electronic System Organization", Article 22* (1) Electronic System Provider must provide an audit trail for all activities of the Electronic System organization. (2) Audit trail as referred to in paragraph (1) is utilized for the purpose of supervision, law enforcement, dispute resolution, verification, testing, and other examinations.	This is a customer consideration. Google offers customers control and monitoring functionality via the Cloud Console in addition to information, audit and access rights. Customers can also use Access Transparency, which is a feature that enables them to review logs of actions taken by Google personnel regarding their data. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).
15.	*Division 7 "Security of Electronic System Organization", Article 23* The Electronic System Provider must conduct security for the components of the Electronic System.	This is a customer consideration. Refer to row 2.
16.	*Division 7 "Security of Electronic System Organization", Article 24* (1) The Electronic System Provider must own and operate procedures and facilities for the security of the Electronic System in preventing disturbance, failure, and loss. (2) The Electronic System Provider must facilitate a security system which covers the procedures and prevention and control system upon a threat and attack which causes a disturbance, failure, and loss. (3) In the event that there is a system failure or disturbance which has a serious impact as a result of other parties action to the Electronic System, the Electronic System Provider must secure the Electronic Information and/or Electronic Document and shall immediately report in the first place to the law enforcement and the relevant Ministry or Body. (4) Further provisions on the security system as referred to in paragraph (2) shall be regulated in regulation of the head of agency who is in charge of governmental affairs in the cybersecurity sector.	This is a customer consideration. Refer to row 2.
17.	*Division 7 "Security of Electronic System Organization", Article 25* The Electronic System Provider must redisplay the Electronic Information and/or Electronic Document as a whole in accordance with the format and retention period which is established based on laws and regulations.	This is a customer consideration.
18.	*Division 7 "Security of Electronic System Organization", Article 26*	This is a customer consideration. Refer to row 2.

Government Regulation No. 71

GCP and Google Workspace Mapping

	(1) The Electronic System Provider must maintain the confidentiality, integrity, authenticity, accessibility, availability, and traceability of Electronic Information and/or Electronic Document in accordance with laws and regulations. (2) In the organization of the Electronic System which is aimed at transferable Electronic Information and/or Electronic Document, the Electronic Information and/or Electronic Document shall be unique as well as explaining its possession and ownership.	Control Customers can provide Google instructions about their data and Google will comply with those instructions based on our contractual commitments. Google commits to only access or use customer data to provide the services ordered by the customer and will not use it for any other Google products, services, or advertising. See Section 5 (Processing of Data) of the DPA and DPST. Ownership Customers retain all intellectual property rights in their data.
19.	*Division 7 "Security of Electronic System Organization", Article 27* The Electronic System Provider shall ensure that the Electronic System functions in accordance with its designation by taking into consideration the interoperability and compatibility with the previous Electronic System and/or the relevant Electronic System.	This is a customer consideration. Google enables customers to access and export their data throughout the duration of their contract and during the post-termination transition term. Customers can export their data from GCP services in a number of industry standard formats. For example: • Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. • Migrate for Anthos allows you to move and convert workloads directly into containers in Google Kubernetes Engine. • Customers can export/import an entire VM image in the form of a .tar archive. Find more information on images and storage options on our Compute Engine Documentation page. Information is also available on our Google Account help page for Google Workspace. In addition, Data Export is a feature that makes it easy to export and download a copy of your data securely from our Google Workspace services. See Section 9 (Access etc.; Data Subject Rights; Data Export) of the DPA and DPST.
20.	*Division 7 "Security of Electronic System Organization", Article 29* The Electronic System Provider must provide information to the Electronic System User at least on: a. identity of the Electronic System Provider; b. the transacted object; c. feasibility or security of the Electronic System; d. procedures for device utilization; e. contract terms;	This is a customer consideration. Google's Terms of Service outline the responsibilities of Google and customers Customers can monitor the performance of their GCP services (including the SLAs) on an ongoing basis using the functionality of the services. For example: • The Status Dashboard provides status information on the Services.

	f. procedures to reach agreement; g. privacy and/or protection of Personal Data guarantee; and h. phone number of the complaint center.	• Cloud Security Command Center and Security Health Analytics provide visibility and monitoring of Google Cloud Platform resources and changes to resources including VM instances, images, and operating systems. • Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. Customers can monitor Google's performance of Google Workspace services (including the SLAs) on an ongoing basis using the functionality of the services. For example: • The Status Dashboard provides status information on the Services. • Admin Console Reports allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. • Access Transparency is a feature that enables you to review logs of actions taken by Google personnel regarding your user content. Log entries include: the affected resource, the time of action, the reason for the action (e.g. the case number associated with the support request); and data about who is acting on data (e.g. the Google personnel's location).
21.	*Division 7 "Security of Electronic System Organization", Article 30* (1) The Electronic System Provider must provide features in accordance with the characteristics of the utilized Electronic System. (2) Features as referred to in paragraph (1) shall at least in the form of facilities to: a. make correction; b. cancel a command; c. provide a confirmation or reconfirmation; d. choose to continue or to stop the next activity; e. view the submitted information in the form of Electronic Contract offers or advertisement; f. check the success or failure of an Electronic Transaction; and g. read an agreement before conducting an Electronic Transaction.	This is a customer consideration. The different service offerings provided by Google are described on our services summary page here (GCP) and here (Google Workspace). Customers decide which services to use, how to use them and for what purpose. Google provides functionality to enable customers to access, rectify, and restrict processing of their data as well as retrieve or delete data. See Section 9 (Access etc.; Data Subject Rights; Data Export) of the DPA and DPST.
22.	*Division 7 "Security of Electronic System Organization", Article 31*	This is a customer consideration. Refer to Row 12.

Government Regulation No. 71

GCP and Google Workspace Mapping

	The Electronic System Provider must protect its user and public from loss due to the organized Electronic System.	
23.	*Division 7 "Security of Electronic System Organization", Article 32* (1) Any person who works within the Electronic Systems organization must secure and protect the facilities and infrastructure of Electronic System or information which are distributed through the Electronic System. (2) The Electronic System Provider must provide, educate, and train the personnel whose duties and responsibilities are concerned with the security and protection of facilities and infrastructure of the Electronic System.	This is a customer consideration. Refer to Rows 2 and 11. All Google employees undergo security training as part of the orientation process and receive ongoing security training throughout their Google careers. During orientation, new employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on their job role, additional role-specific privacy and security training may be required. For instance, the information security team instructs new engineers on topics like secure coding practices, product design, and automated vulnerability testing tools. Privacy and security training are also required annually. See Appendix 2 (Security Measures) section 4 (Personnel Security) of the DPA and DPST.
24.	*Division 7 "Security of Electronic System Organization", Article 33* For the purpose of criminal justice process, the Electronic System Provider must provide the Electronic Information and/or Electronic Data which are contained in the Electronic System or Electronic Information and/or Electronic Data which are processed by the Electronic System at a valid request from an investigator for certain criminal act in accordance with the authority regulated in laws.	This is a customer consideration. Google understands that this is important and is committed to maintaining trust with customers by being transparent about how we respond to government requests if received. If Google receives a government request, Google will: ● attempt to redirect the request to the customer ● notify the customer prior to disclosure unless prohibited by law ● comply with the customer requests to oppose disclosure ● only disclose if strictly necessary to comply with legal process More information about Google's practices around government requests for data is available in our Government Requests for Cloud Customer Data whitepaper. To provide even more transparency, Google reports the government requests we receive for enterprise Cloud customers in our Enterprise Cloud Transparency Report.
25.	*Division 8 "Feasibility Test for Electronic System", Article 34* (1) The Electronic System Provider must conduct a Feasibility Test for Electronic System. (2) The obligation as referred to in paragraph (1) may be implemented to all components or parts of components in the Electronic System in accordance with the characteristics of the needs for protection and strategic nature of the organization of the Electronic System.	This is a customer consideration.

Government Regulation No. 71

GCP and Google Workspace Mapping

26.	*Division 9 "Supervision", Article 35* (1) The Minister is authorized to conduct supervision upon the organization of the Electronic System. (2) The supervision as referred to in paragraph (1) shall consist of monitoring, controlling, examination, searching, and security. (3) The provisions on supervision for the organization of Electronic systems in certain sectors must be established by the relevant Ministry or Body after coordinating with the Minister.	This is a customer consideration. Refer to Row 21.