# KNF - Communication on using cloud computing services

## Google Cloud Mapping

This document is designed to help supervised entities regulated by the KNF (“**regulated entity**”) to consider the KNF Communication of 23 January 2020 on information processing by supervised entities using public or hybrid cloud computing services (the “**framework**”) in the context of Google Cloud Platform (“**GCP**”) and the Google Cloud Financial Services Contract.

We focus on the following requirements of the framework: VII. Minimum requirements for cloud-based information processing, paragraphs 1-4 and 6-8. For each section, we provide commentary to help you understand how you can address the requirements using the Google Cloud services and the Google Cloud Financial Services Contract.

| # | Framework reference | | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|---|
| **VII. Minimum requirements for cloud-based information processing** | | | | |
| 1. | 1. | These minimum technical and organisational requirements for cloud-based information processing represent a reference that the supervised entity should verify for the appropriateness for the results of risk assessment and to ensure that the requirements are fulfilled. | Google recognizes that you need to perform a risk assessment before deciding to use our services. To assist you, we’ve provided information for each of the areas you need to consider in the rows that follow. | N/A |
| 2. | 2. | The technical means and organisational resources use to ensure information security should result from the completed risk assessment process but – regardless of the results of such assessment – they must not ‘soften’ the above requirements. | This is a customer consideration. | N/A |
| 3. | **3.** | **Ensuring competence** | | |
| 4. | 3.1. | The supervised entity should ensure, in a documented process, appropriate competences for the intended or ongoing information processing operations in a cloud computing environment. The competences should result from the requirements concerning education, training, skills and experience of the supervised entity’s employees and collaborators engaged in the planning, implementation, testing and maintenance of cloud-based information processing, and the requirements to conclude and review the related agreement. | This is a customer consideration. | N/A |
| 5. | 3.2. | The supervised entity should also ensure proper understanding of the consequences of using a certain cloud computing architecture, the configuration rules, the distribution of responsibility for information security, according to the scope and type of the intended or existing cloud computing environment and the service model, considering the requirements on business continuity for the supervised entity and its IT infrastructure. The understanding of consequences of a given choice should be reflected in the risk assessment documentation, the guarantee of appropriate resources both in qualitative and quantitative terms as well as in all the works (and agreements) related to the development or upgrade of software to be used in the cloud and in the integration of services based on the supervised entity’s own resources. | Understanding the services<br><br>Information about Google Cloud’s technology and systems architecture is available on our Choosing Google Cloud page.<br><br>Information on configuration management is available on our Configuration Management page.<br><br>For more information on:<br>• information security refer to Rows 9 and 52,<br>• business continuity refer to Row 9, and<br>• upgrades of software refer to Row 23.<br><br>Integration<br><br>There are a number of ways to integrate our services with your systems. | N/A |

# KNF - Communication on using cloud computing services

## Google Cloud Mapping

| # | Framework reference | | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|---|
| | | | • **Cloud Console** allows you to find and check the health of all your Google Cloud resources in one place, including virtual machines, network settings, and data storage.<br>• **Cloud APIs** allow you to access Google Cloud products from your code and automate your workflows by using your preferred programming language. | |
| 6. | 3.3. | The competences of the supervised entity's employees and/or collaborators responsible for security and planning, configuration, management and monitoring of cloud services should be confirmed by an appropriate training documentation and personal certificates regarding the relevant scope of the applicable cloud services (or they should follow from the skills and experience), including specific services or services configured specifically to the relevant cloud service provider. That requirement also applies to the competences of individuals responsible for the review or verification of audit documents, certificates and other documents of the cloud service provider, including agreement for the provision of the cloud service as well as technical documents. | Google provides documentation to explain how regulated entities and their employees can use our services. If a regulated entity would like more guided training, Google also provides a variety of courses and certifications. | N/A |
| 7. | **4.** | **Agreement with the cloud service provider** | | |
| 8. | 4.1. | The supervised entity should have a formal agreement (and other documents, including statements, rules, terms of use, including in electronic version) with the cloud service provider which – where appropriate in relation to the services and scope of information processing – contains or indicates a source of information about: | The Google Cloud Financial Services Contract is the formal agreement between the parties. | N/A |
| 9. | 4.1(a) | a clear distribution of responsibility for information security, considering the service model, the service continuity (including the RTO and RPO[4] parameters, where appropriate) and declared SLA together with the measurement and reporting method<br><br>[4] RTO – Recovery Time Objective, the time from a failure of an IT system until its recovery. RPO – Recovery Point Objective, maximum length of time from the last data backup until a failure of the cloud service. This also means a potential risk (accepted by the supervised entity) that the results of information processing might be lost for a specified duration of time.; | Information security<br><br>This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security.<br><br>The security of a cloud service consists of two key elements:<br><br>(1) Security of Google's infrastructure<br><br>Google manages the security of our infrastructure. This is the security of the hardware, software, networking and facilities that support the Services.<br><br>Given the one-to-many nature of our service, Google provides the same robust security for all our customers. | Data Security; Security Measures (Cloud Data Processing Addendum) |

# KNF - Communication on using cloud computing services

## Google Cloud Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | 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.<br><br>More information is available at:<br><br>● Our infrastructure security page<br>● Our security whitepaper<br>● Our cloud-native security whitepaper<br>● Our infrastructure security design overview page<br>● Our security resources page<br><br>In addition, you can review Google's SOC 2 report. Refer to Row 33.<br><br>(2) Security of your data and applications in the cloud<br><br>You define the security of your data and applications in the cloud. This refers to the security measures that you choose to implement and operate when you use the Services.<br><br>(a) Security by default<br><br>Although we want to offer you as much choice as possible when it comes to your data, the security of your data is of paramount importance to Google and we take the following proactive steps to assist you:<br><br>● **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.<br><br>● **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.<br><br>(b) Security products<br><br>In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our Cloud Security Products page. | |

# KNF - Communication on using cloud computing services

## Google Cloud Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | (c) Security resources<br><br>Google also publishes guidance on:<br><br>• Security best practices<br>• Security use cases<br><br>Service Continuity<br><br>Google will implement a business continuity plan for the Services, review and test it at least annually and ensure it remains current with industry standards. Regulated entities can review our plan and testing results.<br><br>In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide. In particular, refer to the Architecting disaster recovery for cloud infrastructure outages article for information about how you can achieve your desired RTO and RPO for your applications.<br><br>SLA<br><br>The SLAs are available on our Google Cloud Platform Service Level Agreements page.<br><br>You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.<br><br>For example:<br><br>• The Status Dashboard provides status information on the Services.<br><br>• Google Cloud Operations is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. | Business Continuity and Disaster Recovery<br><br>Services<br><br>Ongoing Performance Monitoring |

# KNF - Communication on using cloud computing services

## Google Cloud Mapping

| # | Framework reference | | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|---|
| 10. | 4.1(b) | a clear definition and indication of location[5] of information processing and verification as well as securing compliance through at least a reference to appropriate documents, description of configuration, methods and tools;<br><br>[5] A precise indication of location of the data processing centre (DPC) may pose a threat to the physical security of information but, as a minimum, one should use terms such as 'availability zone', 'region' or any other equivalent term, specifying at least the country and approximate location of the DPC, which terms are used by the cloud service provider in the standard communication, e.g. by specifying the city/town or region of the country. Where such specification is not possible or – due to the scale of activities and the number of locations where information is processed – inappropriate, an EEA area (for the European Economic Area) or any other equivalent description should be provided. | Location of data processing<br><br>To provide you with a fast, reliable, robust and resilient service, Google may store and process your data where Google or its subprocessors maintain facilities.<br><br>• Information about the location of Google's facilities and where individual GCP services can be deployed is available here.<br>• Information about the location of Google's subprocessors' facilities is available here.<br><br>Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. In particular:<br><br>• The same robust security measures apply to all Google facilities, regardless of country / region.<br>• Google makes the same commitments about all its subprocessors, regardless of country / region.<br><br>Securing compliance<br><br>Google provides you with choices about where to store your data - including a choice to store your data in Europe. Once you choose where to store your data, Google will not store it outside your chosen region(s).<br><br>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 European customers on Google Cloud Whitepaper. | Data Center Location; Data Transfers (Cloud Data Processing Addendum)<br><br>Data Security; Subprocessors (Cloud Data Processing Addendum)<br><br>Data Location (Service Specific Terms) |
| 11. | 4.1(c) | the governing law of the agreement (including the competent court and dispute resolution rules); | Refer to your Google Cloud Financial Services Contract. | Governing Law |
| 12. | 4.1(d) | confirmation of compatibility of personal data processing with the EU legislation, if applicable; | Google will comply with all data protection regulations applicable to it in the provision of the Services, including the GDPR.<br><br>In addition, Google makes commitments to protect your data, including regarding security, access and transfer in the Cloud Data Processing Addendum. | Representations and Warranties |
| 13. | 4.1(e) | ownership of information during the term and after termination (expiration, dissolution) of the agreement, even if unplanned; | You retain all intellectual property rights in your data, the data you derive from your data using our services and your applications, both during the term and after termination. | Intellectual Property |

# KNF - Communication on using cloud computing services

## Google Cloud Mapping

| # | Framework reference | | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|---|
| 14. | 4.1(f) | guarantees, implied warranties, insurance (insurance policy of the cloud service provider), liquidated damages, definition of force majeure, events treated as force majeure, and the procedures to be followed in such situations, if applicable; | Warranties<br><br>Refer to your Google Cloud Financial Services Contract.<br><br>Force Majeure<br><br>Refer to your Google Cloud Financial Services Contract.<br><br>Insurance<br><br>Google will maintain insurance cover against a number of identified risks. | Representations and Warranties<br><br>Force Majeure<br><br>Insurance |
| 15. | 4.1(g) | definition of the scope of responsibility for damage caused to the customers of the supervised entity (if applicable), in accordance with the legal requirements imposed on the supervised entity; | Refer to your Google Cloud Financial Services Contract. | Liability |
| 16. | 4.1(h) | a clear indication of subvendors (name, location, scope of operations) of the cloud service provider and the requirements for granting rights of access to information processed by the supervised entity; | Subvendors<br><br>To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will:<br><br>• provide information about our subvendors (including their name, function and location);<br>• provide advance notice of changes to our subvendors; and<br>• give regulated entities the ability to terminate if they have concerns about a new subvendor.<br><br>Subvendor access<br><br>Google ensures via a written contract that subvendors only access customer data to the extent required to perform the obligations subcontracted to them and in accordance with our customer contracts. For more information about Google's data access processes and policies refer to the Access Policy described in Appendix 2 (Security Measures) of the Cloud Data Processing Addendum. | Google Subcontractors<br><br>Subprocessors (Cloud Data Processing Addendum) |
| 17. | 4.1(i) | a clear indication of the rules according to which the tasks and the scope of authorisation, responsibility and accountability of subvendors of the cloud service provider are transparent and clearly identified by the supervised entity; | Google requires our subvendors to meet the same high standards that we do. In particular, Google requires our subvendors to comply with our contract with you. Google will remain accountable to you for the performance of all subcontracted obligations. | Google Subcontractors |

# KNF - Communication on using cloud computing services

## Google Cloud Mapping

| # | Framework reference | | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|---|
| 18. | 4.1(j) | sources of authorised information on the expected changes in the standards applicable to the relevant cloud services (including technical changes); | For more information on how we communicate changes to the service refer to Row 23. | N/A |
| 19. | 4.1(k) | the sources of technical documentation and declarations of conformity (including compliance with applicable laws), and cloud service configuration manuals; | Technical documentation<br><br>Refer to our Documentation page for technical documentation, including information on service configuration. In addition, **Cloud Deployment Manager** enables you to create and manage cloud resources with simple templates to parameterize the configuration.<br><br>Declarations of conformity<br><br>For more information on the certifications and third party audit reports Google provides refer to Row 33. | N/A |
| 20. | 4.1(l) | the scope of additional information and documentation submitted by the cloud service provider in connection with the provision of the cloud service; | Refer to Row 33 for the documentation made available by Google. | N/A |
| 21. | 4.1(m) | the supervised entity's right to conduct inspections at locations where information is processed, including the right to conduct an audit of the other party or third party at the request of the supervised entity (provided this is required following risk assessment); | Google recognizes that regulated entities must be able to audit our services effectively. Google grants audit, access and information rights to regulated entities and supervisory authorities, and both their appointees. This includes access to Google's premises used to provide the Services to conduct an on-site audit.<br><br>Google will ensure our subvendors comply with our contract with you, including the audit and access rights. | Customer Information, Audit and Access<br><br>Google Subcontractors |
| 22. | 4.1(n) | the Supervisor's right to perform inspection duties, e.g. to check the premises and the documentation pertaining to the processing of information of the supervised entity, the processes and procedures, the organisation, management and certificates of compliance; | Google grants the same audit, access and information rights to supervisory authorities and their appointees as we grant to regulated entities. This includes access to Google's premises used to provide the Services to conduct an on-site audit. | Regulator Information, Audit and Access |
| 23. | 4.1(o) | the licensing rules (including the right to update the security of software or its components) and intellectual property rights, including – if applicable – the right to handle information which is being processed; | Updates to the Service<br><br>Google continuously updates the services to enable our customers to take advantage of the most up-to-date technology. Given the one-to-many nature of our service, updates apply to all customers at the same time.<br><br>Google will not make updates that materially reduce the functionality, performance, availability or security of the Services. If Google needs to discontinue a service without replacing it, you will receive at least 12 months' advance notice. Google will continue to provide support and product and security updates during this period. | Changes to Services |

# KNF - Communication on using cloud computing services

## Google Cloud Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | Use of your information<br><br>Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising.<br><br>For more information on intellectual property rights and ownership of data refer to Row 13. | Protection of Customer Data |
| 24. | 4.1(p) the rules for amending the agreement, including the technical parameters of the relevant cloud services; | As services and technology change, Google may update certain terms at URLs that apply to all our customers. Any updates must meet strict criteria. For example, they must not result in a material degradation of the overall security of the services or have a material adverse impact on your existing rights. Beyond these limited updates, any contract changes must be made in writing and signed by both parties. | Changes to Terms; Amendments |
| 25. | 4.1(q) the rules for terminating the agreement, including the rules and time limits for deleting information which is being processed; | Regulated entities can elect to terminate our contract for convenience with advance notice, including if necessary to comply with law.<br><br>In addition, regulated entities may terminate our contract with advance notice for Google's material breach after a cure period, for change in control or for Google's insolvency. | Term and Termination |
| | | Google recognizes that regulated entities need sufficient time to exit our services (including to transfer services to another service provider). To help regulated entities achieve this, upon request, Google will continue to provide the services for 12 months beyond the expiry or termination of the contract.<br><br>Google will enable you to access and export your data throughout the duration of our contract and during the post-termination transition term. You can export your data from the Services in a number of industry standard formats. For example:<br><br>• **Google Kubernetes Engine** is a managed, production-ready environment that allows portability across different clouds as well as on premises environments.<br><br>• **Migrate for Anthos** allows you to move and convert workloads directly into containers in Google Kubernetes Engine. | Transition Term |

# KNF - Communication on using cloud computing services

## Google Cloud Mapping

| # | Framework reference | | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|---|
| | | | • You 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.<br><br>On termination of the contractual relationship, Google will comply with your instruction to delete Customer Data from Google systems. | Deletion on Termination (Cloud Data Processing Addendum) |
| 26. | 4.1(r) | the rules regarding support, including the scope and time slots (e.g. time zones), the methods and procedures for reporting issues with cloud services; | The support services are described on our technical support services guidelines page. | Technical Support |
| 27. | 4.1(s) | the rules for sharing information, including in particular regarding safety and management of current incidents, applicable to both the staff of the supervised entity and of the cloud service provider, and – in the case of material exposure to the impact of a given incident – also to other parties (e.g. customers, subvendors), to ensure the appropriateness of procedures to the weight of the incident. | Google will make information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to you. More information is available on our Incidents & the Google Cloud dashboard page.<br><br>In addition, Google will notify you of data incidents promptly and without undue delay. More information on Google's data incident response process is available in our Data incident response whitepaper. | Significant Developments<br><br>Data Incidents (Cloud Data Processing Addendum) |
| 28. | 4.2. | Without prejudice to legal requirements or to this communication, the supervised entity may use framework agreement forms made available by the cloud service provider, especially where the agreement concerns cloud services developed for a group of entities (including the supervised entity) as part of corporate or group agreements, including community cloud services. In that case, the supervised entity should: | The Google Cloud Financial Services Contract is designed to address requirements applicable to regulated entities and is available to regulated entities. | N/A |
| 29. | 4.2(a) | determine to what extent the framework agreement and related documents, the results of risk assessment as well as the legal, organisational and technical requirements take into account the provisions of this communication and are appropriate for the supervised entity's circumstances and intentions regarding cloud-based information processing; | This is a customer consideration. | N/A |
| 30. | 4.2(b) | assess if it is necessary and possible to apply the requirements of this communication independently, to the extent that is incompatible with the framework agreement and related documents. | This is a customer consideration. | N/A |
| 31. | **6.** | **Requirements for cloud service providers[6]** | | |
| 32. | [Footnote] | [6] The requirements should be considered by the supervised entity in its approach to the application of cloud services, in particular in risk assessment. | | |

# KNF - Communication on using cloud computing services

## Google Cloud Mapping

| # | Framework reference | | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|---|
| 33. | 6.1. | According to the actual scope and scale of the cloud services, the cloud service provider should meet the requirements for compliance with the following standards or their equivalents in the Polish or European standardisation system, unless the supervised entity accepts (based on the results of risk assessment) that it is not necessary to meet such requirement in whole or in part:<br><br>(a) PN-ISO/IEC ISO 20000 on IT service management;<br>(b) PN-EN ISO/IEC 27001 on information security management;<br>(c) PN-EN ISO 22301 on service continuity management;<br>(d) ISO/IEC 27017 on cloud information security;<br>(e) ISO/IEC 27018 on the code of practice for protection of personally identifiable information (PII) in clouds. | Google recognizes that you 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. Google commits to comply with the following key international standards during the term of our contract with you:<br><br>• ISO/IEC 27001:2013 (Information Security Management Systems)<br>• ISO/IEC 27017:2015 (Cloud Security)<br>• ISO/IEC 27018:2014 (Cloud Privacy)<br>• PCI DSS<br>• SOC 1<br>• SOC 2<br>• SOC 3<br><br>You can review Google's current certifications and audit reports at any time. | Certifications and Audit Reports |
| 34. | 6.2. | The DPC of the cloud service provider should meet the requirements of PN-EN 50600 (Data centre facilities and infrastructures) as a minimum for Class 3 or ANSI/TIA-942 for Tier III, or any other appropriate recognised standard for the evaluation of DPCs, or any DPC-related standard, and the supervised entity may accept (in duly justified cases and following risk assessment) non-compliance with certain requirements. | Google data centers feature a layered security model with custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics.<br><br>For more information on our data centers refer to our our infrastructure security page and our infrastructure security design overview page. In addition, you can review Google's SOC 2 report. | Certifications and Audit Reports |
| 35. | 6.3. | The Supervisor recommends that the DPC should be located in the territory of an EEA country. This provision is subject to the rule that the supervised entities that: | Google has multiple data centers in the EEA. Information about the location of Google's facilities and where individual GCP services can be deployed is available here.<br><br>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 European customers on Google Cloud Whitepaper. | N/A |
| 36. | 6.3(a) | have been recognised, by decision, as key service operators as defined in Article 5(2) of the Act of 5 July 2018 on the national cybersecurity system, and that use a cloud service to deliver a key service, or | This is a customer consideration. | N/A |
| 37. | 6.3(b) | are critical infrastructure operators as defined in the Act of 26 April 2007 on crisis management, and that use a cloud service to perform the tasks of critical infrastructure operation | This is a customer consideration. | N/A |
| 38. | 6.3 (continued) | should use, in the first place, the DPCs located in the territory of the Republic of Poland, unless – in the supervised entity's view – the proposed contractual, financial, operational, SLA-related or functional terms and conditions are at least as good as those applicable to the DPCs located outside the territory of the Republic of Poland. | Google provides the same contractual commitments and technical and organizational measures for your data regardless of the country / region where it is located. | N/A |

# KNF - Communication on using cloud computing services

## Google Cloud Mapping

| # | Framework reference | | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|---|
| 39. | 6.4. | A cloud service provider should ensure, as part of its rules of procedure, a documented rule for protection of information processed by the supervised entity against unauthorised access or use by the entity's staff or subvendors, at least by: | | |
| 40. | 6.4(a) | applying a default rule of no access to information processed by the supervised entity; | For more information on access management refer to Row 43. | N/A |
| 41. | 6.4(b) | applying a default rule of no administrator or user account on virtual machines of the supervised entity or in any cloud services that are being launched; | For more information on security products you can use to monitor the security of your data and access management refer to Row 9 and 43. | N/A |
| 42. | 6.4(c) | applying the rule of the 'necessary minimum' requirements for service account rights, to be granted only where it is necessary to perform operations required by the supervised entity (e.g. troubleshooting) and only for the duration of such operations, based on a service request made by the supervised entity; the whole management and execution process may be carried out after log-in; The applicable operation procedures may also be confirmed by a relevant certificate (e.g. SOC[7] 2 Type 2) issued by an independent certification body accredited in line with the European accreditation standards;<br><br>[7] System and Organization Controls | The "Managing Google's Access to your Data" section of our Trusting your data with GCP whitepaper explains Google's data access processes and policies.<br><br>In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools:<br><br>• **Access Transparency** is a feature that enables you to review logs of actions taken by Google personnel regarding your 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).<br>• **Access Approval** is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency.<br><br>For more information on the third party audit reports Google provides refer to Row 33. | N/A |
| 43. | 6.4(d) | making available guidelines, model configuration, descriptions of rules, etc., which should clearly define separation in information processing and indicate methods of verifying the correctness of configuration; | Google makes available reference architectures, in-depth tutorials and best practices on our Technical Guides page.<br><br>In addition, you can use the following tools to effectively manage how you deploy our services:<br><br>• **Cloud Identity and Access Management** helps to prevent against unauthorized access by controlling access rights and roles for Google Cloud Platform resources. | N/A |

# KNF - Communication on using cloud computing services

## Google Cloud Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | • **Resource Manager** allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources.<br>• **Cloud Deployment Manager** is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources.<br><br>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 European customers on Google Cloud Whitepaper. | |
| 44. | 6.4(e) launching a new default environment (or cloud service) separated from other tenants, with 'secure-by-default' settings[8]<br><br>[8] A default configuration of a cloud service which considers the requirements for security of information processing, mainly to prevent accidental (unintended) disclosure of information that is being processed. | In addition to the other tools and practices available to you outside Google, you can choose to use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available here.<br><br>Here are some examples:<br>• **Cloud Security Scanner** automatically scans App Engine, Compute Engine, and Google Kubernetes Engine apps for common vulnerabilities.<br>• **Event Threat Detection** automatically scans various types of logs for suspicious activity in your Google Cloud Platform environment.<br>• **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.<br>• **Forseti** is an open source toolkit designed to help give your security teams the confidence and peace of mind that they have the appropriate security controls in place across our services. Forseti includes the following security tools:<br>  ○ Inventory: provides visibility into existing GCP resources<br>  ○ Scanner: validates access control policies across GCP resources<br>  ○ Enforcer: removes unwanted access to GCP resources<br>  ○ Explain: analyzes who has what access to GCP resources. | N/A |

# KNF - Communication on using cloud computing services

## Google Cloud Mapping

| # | Framework reference | | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|---|
| | | | For more information, see here. | |
| 45. | 6.5. | The fulfilment of the requirements may be confirmed with appropriate certificates of conformity issued by independent certification bodies accredited in line with the European accreditation standards. | For more information on the certifications and third party audit reports Google provides refer to Row 33. | N/A |
| 46. | **7.** | **Cryptography** | | |
| 47. | 7.1. | The supervised entity should ensure that information processed in a cloud is encrypted in accordance with the rules laid down in this communication. In particular, the supervised entity should make sure that: | Encryption is central to Google's comprehensive security strategy. We provide certain encryption by default, with no additional action required from you. We also offer a continuum of encryption key management options to meet your needs. | N/A |
| 48. | 7.1(a) | it has access to up-to-date detailed cloud configuration manuals and methods of verification of the correctness of configuration and operation, in particular in the area of encryption; | Refer to our Choosing an Encryption Option page for help to identify the solutions that best fit your requirements for key generation, storage, and rotation. | N/A |
| 49. | 7.1(b) | it has adequate competences to set up proper configuration of cloud services in line with the guidelines submitted by the cloud service provider, including in terms of encryption; | This is a customer consideration. | N/A |
| 50. | 7.1(c) | it uses dedicated configuration settings – or settings recommended by the cloud service provider – that increase the safety of the cloud services concerned; | This is a customer consideration. Refer to Row 48 for more information on the help Google provides to identify the solutions that best fit your requirements for key generation, storage, and rotation. | N/A |
| 51. | 7.1(d) | information protected by law is encrypted both as data 'at rest' and data 'in transit.' | Encryption at rest<br><br>Google encrypts customer data stored at rest by default, with no additional action required from you. More information is available on the Google Cloud Encryption at rest page.<br><br>Encryption in transit<br><br>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 on the Google Cloud Encryption in transit page. | N/A |
| 52. | 7.2. | The supervised entity should ensure that information is encrypted with the keys generated and managed by the supervised entity, unless the risk assessment shows that it is acceptable or advisable to use encryption keys generated or managed by the cloud service provider | We know you need control over who can access your data. Refer to our Engaging in a European dialogue on customer controls and open cloud solutions blog post for a summary of the steps we're taking to address this important requirement, including regarding encryption. | N/A |

# KNF - Communication on using cloud computing services

## Google Cloud Mapping

| # | Framework reference | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|
| | | You can choose to use these encryption and key management tools provided by Google:<br><br>• Cloud KMS is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on-premises.<br><br>• Cloud HSM is a cloud-hosted key management service that lets you protect encryption keys and perform cryptographic operations within a managed HSM service. You can generate, use, rotate, and destroy various symmetric and asymmetric keys.<br><br>• Customer-managed encryption keys for Cloud SQL and GKE persistent disks.<br><br>• Cloud External Key Manager (beta) lets you protect data at rest in BigQuery and Compute Engine using encryption keys that are stored and managed in a third-party key management system that's deployed outside Google's infrastructure.<br><br>• Key Access Justification (alpha) works with External Key Manager. It provides a detailed justification each time one of your keys is requested to decrypt data, along with a mechanism for you to explicitly approve or deny providing the key using an automated policy that you set. | |
| 53. | 7.3. Where the risk assessment reveals the need to keep and manage encryption keys when using hardware security modules (HSM[9] ), the HSMs may be provided by the cloud service provider, considering that element in the risk assessment. The HSMs should meet the requirements of FIPS[10] 140-2 Level 2 or equivalent.<br><br>[9] HSM – Hardware Security Module, a device that safeguards and manages cryptographic keys<br>[10] Federal Information Processing Standard – publicly announced standards for the U.S. non-military government agencies. In this context: an international standard for security of cryptographic modules. | Refer to Row 52. | N/A |
| 54. | 7.4. The supervised entity should have in place a documented process to manage and control the generation, use (including access rules), protection and destruction of keys. | Refer to Row 52. | N/A |

# KNF - Communication on using cloud computing services

## Google Cloud Mapping

| # | Framework reference | | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|---|
| 55. | 7.5. | The encryption key management process should include keeping, within one's own infrastructure, copies of the encryption keys that have been generated or managed by the cloud service provider and are used in special cloud-based outsourcing, unless the risk assessment has shown that this is not necessary. | Refer to Row 52. | N/A |
| 56. | **8.** | **Monitoring information processing in the cloud computing environment** | | |
| 57. | 8.1. | The supervised entity should have in place documented rules for collecting logs relating to cloud-based information processing, according to the scope of cloud services, information that is being processed, and the results of risk assessment. | Google recognizes that you need visibility into who did what, when, and where for all user activity on our service.<br><br>**Google Cloud Operations** is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. In particular, **Cloud Audit Logs** help your security teams maintain audit trails in GCP and view detailed information about Admin activity, data access, and system events.<br><br>In addition, for more information about how you can monitor and control the limited actions performed by Google personnel on your data refer to Row 42. | N/A |
| 58. | 8.2. | The supervised entity should protect the logs against unauthorised access, modification or deletion for a period of time specified in the security rules following from the risk assessment and the applicable special rules. | **Cloud Audit Logs** are encrypted at rest by default and reside in highly protected storage, resulting in a secure, immutable, and highly durable audit trail. The service is also coupled with Google Cloud's **Access Transparency** service, which surfaces near real-time logs of GCP administrator access to your systems and data. | N/A |
| 59. | 8.3. | Authorised members of the supervised entity's staff should review the logs in accordance with the documented security rules and procedures, and – depending on the scale of activity, type and number of incidents logged, and the security architecture – the Supervisor recommends the use of specialised software to correlate log data on events (Security Information and Event Management – SIEM) as well as a regular review and update of correlation rules | This is a customer consideration. | N/A |
| 60. | 8.4. | Requirements applicable to the supervised entity in the area of management of service providers that have remote access to the cloud services used by the supervised entity[11]:<br><br>[11] The requirements apply to a situation where a supervised entity orders its service provider to carry out operations on the supervised entity's resources uploaded to the cloud (e.g. to update software or to carry out servicing work). The requirements do not apply to the support services offered by the | | |

# KNF - Communication on using cloud computing services

## Google Cloud Mapping

| # | Framework reference | | Google Cloud commentary | Google Cloud Financial Services Contract reference |
|---|---|---|---|---|
| | | cloud service provider in respect of the servicing standards under the agreement for the provision of the cloud service. | | |
| 61. | 8.4(a) | the supervised entity should ensure that specific IT systems and/or specific parts of the IT structure may only be accessed by the authorised staff of the service provider; | This is a customer consideration. For more information about how you can monitor and control the limited actions performed by Google personnel on your data refer to Row 42. | N/A |
| 62. | 8.4(b) | the supervised entity should require that the service provider's staff use multi-factor authentication (MFA), with the type and scope being determined by the results of the risk assessment; | This is a customer consideration. Google provides a wide variety of MFA verification methods to help protect your user accounts and data. Refer to our Multi-Factor Authentication page for more information. | N/A |
| 63. | 8.4(c) | the supervised entity should ensure that administrative and privileged user access is restricted to trusted networks of the supervised entity and/or service provider and controlled (including by recording sessions and session parameters, and then by analysing the correctness and purpose of each operation), unless the risk assessment has shown that this is not necessary. | This is a customer consideration. At Google we rely on a zero trust system known as BeyondCorp, to move beyond the idea of a privileged corporate network. For more information on our zero trust approach refer to our What is Zero Trust Identity Security? blog post. | N/A |