ACPR - Order of 3 November 2014

Google Cloud Mapping

This document is designed to help obligated companies supervised by the ACPR ("**regulated entity**") to consider Chapter II of Title V of the Order of 3 November 2014 (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: Articles 238 and 239. For each paragraph, 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
1.	Art 238 Outsourcing activity:		
2.	(a) Gives rise to an assessment of the risk incurred prior to the signing of the contract;	Google recognizes that you need to conduct due diligence and perform a risk assessment before deciding to use our services. To assist you, we've provided the information below. You can review Google's current certifications and audit reports at any time. Compliance reports manager provides you with easy, on-demand access to these critical compliance resources.	Certifications and Audit Reports
3.	(b) Gives rise to a written contract between the external service provider and the obligated company;	The Google Cloud Financial Services Contract is the formal agreement between the parties.	N/A
4.	(c) Is part of a formalised policy of control of external providers defined by the obligated company. Appropriate measures are taken if it appears that the service provider may not perform its duties effectively or in accordance with legislative or regulatory requirements;	The SLAs provide measurable performance standards and remedies for the services and are available on our Google Cloud Platform Service Level Agreements page. If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits. You can monitor Google's performance of the Services (including the SLAs) on a regular basis using the functionality of the Services. For example: • The **Status Dashboard** provides status information on the Services. • Google Cloud **Operations** is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP. • **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).	Services Ongoing Performance Monitoring

ACPR - Order of 3 November 2014

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
5.	(d) May be suspended if necessary without affecting the continuity or quality of the services provided to clients.	<u>Cease use of service</u> If you wish to stop using our services you may do so at any time. <u>Transition</u> Google recognizes that regulated entities need to be able to exit our Services without undue disruption to their business, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of their service to their own clients. 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 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: • 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. • 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	Ceasing Services Use Transition Term Data Export (Cloud Data Processing Addendum)
6.	The obligated companies keep and update a register of the externalization arrangements in force, distinguishing between the externalization arrangements relating to essential or important provision of services or operational tasks and the externalization arrangements for other activities.	The regulated entity is best placed to decide if an externalization arrangement relates to an essential or important function. You decide which services to use, how to use them and for what purpose. Therefore, you decide the scope of the arrangement.	N/A
7.	Art 239 Obligated companies ensure, in their relations with their external service providers, that the provider:		
8.	(a) Commit to a level of quality consistent with the normal operation of the service and, in the event of an incident, leading to the use of the back-up mechanisms mentioned in (c);	The SLAs are available on our Google Cloud Platform Service Level Agreements page. For information on how Google responds to incidents refer to Row 12.	Services

ACPR - Order of 3 November 2014

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
9.	(b) Protect confidential information relating to the obligated company and its clients;	This is addressed in the Cloud Data Processing Addendum where Google makes commitments to protect your data, including regarding security. The confidentiality and security of a cloud service consists of two key elements: (1) 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 In addition, you can review Google's SOC 2 report. (2) Security of your data and applications in the cloud 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. (a) Security by default 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: ● **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.	Confidentiality Data Security; Security Measures (Cloud Data Processing Addendum)

ACPR - Order of 3 November 2014

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• **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 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. (c) Security resources Google also publishes guidance on: • Security best practices • Security use cases	
10.	(c) Implement back-up mechanisms in the event of serious difficulty affecting continuity of service. Failing this, the obligated companies ensure that their back-up and continuation plan takes into account the impossibility for the external provider to provide services;	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. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide. Regulated entities can use Cloud Storage as part of their backup routine. Refer to our Disaster Recovery Building Blocks and Disaster Recovery Scenarios for Data articles for more information about how you can use the services for data backup.	Business Continuity and Disaster Recovery
11.	(d) Cannot impose a substantial change in the service they provide without the prior consent of the obligated company;	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. 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

ACPR - Order of 3 November 2014

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
12.	(e) Comply with the procedures defined by the obligated company concerning the organisation and implementation of the control of the services they provide;	You operate the services independently without action by Google personnel. You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities. You can use the following functionality to control the Services: ● **Cloud Console:** A web-based graphical user interface that customers can use to manage their GCP resources. ● **gcloud Command Tool:** A tool that provides the primary command-line interface to GCP. A command-line interface is a user interface to a computer's operating system. ● **Google APIs:** Application programming interfaces which provide access to GCP. For more information about Google's security controls and tools refer to Row 7.	N/A
13.	(f) Permit them, whenever necessary, access, where appropriate, on-site, to any information on the services made available to them, in compliance with the regulations on the communication of information;	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. Regulated entities may access their data on the services at any time and may provide their supervisory authority with access.	Regulator Information, Audit and Access Customer Information, Audit and Access
14.	(g) Inform them of any event likely to have a significant impact on their ability to perform outsourced tasks effectively and in compliance with applicable legislation and regulatory requirements;	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. 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. For more information on how you can monitor Google's performance of the Services, refer to Row 3.	Significant Developments Data Incidents (Cloud Data Processing Addendum)
15.	(h) Accept that the Prudential Supervisory and Resolution Authority and any other equivalent foreign authority within the meaning of Articles L. 632-7, L. 632-12 and L. 632-13 of the Monetary and Financial Code have access to information on outsourced activities necessary for the performance of its mission, including on-site.	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

ACPR - Order of 3 November 2014

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference