Austrian FMA – ss.25 Bankwesengesetz (BWG)

Google Cloud Platform Mapping

This document is designed to help credit institutions (“**regulated entities**”) supervised by the Austrian Financial Market Authority (“**supervisory authority**”) to consider the Bankwesengesetz or BWG (“**framework**”) in the context of Google Cloud Platform (“**GCP**”) and the Google Cloud Financial Services Contract.

We focus on the Annex to Section 25 (Outsourcing). 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
Annex to Section 25 (Outsourcing Conditions)			
1.	1. The service provider shall possess the relevant qualifications, capacity, as well as all authorisations required by law to perform the outsourced tasks, services, or activities in a reliable and professional manner;	Qualifications and Capacity • Google Cloud has been providing cloud services for over 10 years, assisting customers across the globe in the financial services, healthcare & life science, retail and public sectors to name a few. More information on Google Cloud’s capabilities is available on our Choosing Google Cloud page. • Google Cloud has been named as a leader in several reports by third party industry analysts. You can read these on our Analyst Reports page. • Information about our referenceable customers (including in the financial services sector) is available on our Google Cloud Customer page. • Information about Google Cloud’s leadership team is available on our Media Resources page. • You can review information about our mission, philosophies and culture on Alphabet’s Investor Relations page. Authorisations Google will comply with all laws and regulations applicable to it in the provision of the Services.	N/A Representations and Warranties
2.	2. the service provider shall perform the outsourced services efficiently; for such purpose, the credit institution shall determine assessment methodologies for the performance of such services;	The SLAs provide measurable performance standards for the services. They are available on the Google Cloud Platform Service Level Agreements page.	Services
3.	3. the service provider shall duly monitor the performance of the outsourced tasks and shall reasonably control any risks associated with such outsourcing;	You can monitor Google’s performance of the 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. • **Google Cloud Operations** is an integrated monitoring, logging, and diagnostics hosted solution that helps you gain insight into your applications that run on GCP.	Ongoing Performance Monitoring

Austrian FMA – ss25. Bankwesengesetz

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• **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).	
4.	4. where doubts exist about whether the service provider is effectively performing tasks in compliance with all applicable legal and administrative provisions, adequate measures shall be initiated;	Cease use of Service If you wish to stop using our services you may do so at any time. Remedies If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits. Termination Regulated entities may terminate our contract with advance notice for Google's material breach after a cure period or if necessary to comply with law.	Ceasing Services Use Services Term and Termination
5.	5. the credit institution must continue to possess the necessary specialist knowledge to effectively monitor the outsourced tasks and to control any risks associated with such outsourcing;	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. Regulated entities 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. In addition, 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. See Row 3 for information on how you can monitor Google's performance of the services.	Instructions Technical Support

Austrian FMA – ss25. Bankwesengesetz

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
6.	6. the service provider shall inform the credit institution without delay about any development that may materially impede its ability to perform the outsourced tasks effectively and in compliance with all applicable legal and administrative provisions;	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.	Significant Developments Data Incidents (Data Processing and Security Terms)
7.	7. the credit institution must be able to terminate the outsourcing agreement if required, without doing so having any negative effect on the continuity and quality of the services provided for its customers;	Regulated entities can elect to terminate our contract for convenience, including if necessary to comply with law, or where directed by the supervisory authority. 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.	Termination for Convenience Transition Term
8.	8. the service provider shall cooperate with the FMA and the Oesterreichische Nationalbank with regard to the outsourced activities;	Google will fully cooperate with supervisory authorities exercising their audit, information and access rights.	Enabling Customer Compliance
9.	9. the credit institution, its bank auditors, the FMA and the Oesterreichische Nationalbank must actually have access to the data related to the outsourced activities and to the service provider's business premises. The FMA and the Oesterreichische Nationalbank must be able to exercise such access rights;	Google recognizes that regulated entities must be able to audit our services effectively. Google grants audit, access and information rights to regulated entities, supervisory authorities and both their appointees. This includes access to Google's premises used to provide the Services to conduct and on-site audit. Regulated entities may access their data on the services at any time and may provide their supervisory authority with access.	Customer Information, Audit and Access Regulator Information, Audit and Access
10.	10. the service provider shall protect all confidential information about the credit institution and its customers;	The 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:	Confidentiality Data Security; Security Measures (Data Processing and Security Terms)

Austrian FMA – ss25. Bankwesengesetz

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• 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 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: • 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 You can review Google's current certifications and audit reports at any time. (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. • **Encryption in transit.** Google encrypts and authenticates all data in transit at one or more network layers when data moves outside physical boundaries not	

Austrian FMA – ss25. Bankwesengesetz

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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	
11.	11. the credit institution and the service provider shall establish a contingency plan and ensure continuous compliance with the plan, which guarantees the storage of data in the event of a system failure as well as ensuring the regular testing of backup systems, where so doing is required in light of the outsourced function, service, or activity;	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. Information about how customers can use our Services in their own business contingency planning is available on the Google Cloud Platform Disaster Recovery Planning Guide page. In particular, as part of your contingency planning, you can choose to use build, deploy and optimize your applications in both cloud and on-premises environments. Anthos provides a platform to develop, secure and manage applications across hybrid and multi-cloud environments. 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
12.	12. In the case of outsourcing to a service provider located in a third country, the credit institution shall continually monitor the political, legal and economic developments in the third country, and shall ensure promptly, that any negative developments shall not impede the FMA's performance of its supervisory duties or, in the event that this is not possible, shall notify the FMA of this circumstance without delay, and to revoke the outsourcing arrangement without culpable delay.	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. • Information about the location of Google's facilities and where individual GCP services can be deployed is available on our Global Locations page.	Data Transfers (Data Processing and Security Terms)

Austrian FMA – ss25. Bankwesengesetz

Google Cloud Platform Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page. 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: • The same robust security measures apply to all Google facilities, regardless of country / region. • Google makes the same commitments about all its subprocessors, regardless of country / region. 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). 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 Google will fully cooperate with supervisory authorities exercising their audit, information and access rights regardless of the service location. In addition, regulated entities may access their data on the services at any time and may provide their supervisory authority with access. These rights apply regardless of where the data are stored.	Data Security; Subprocessors (Data Processing and Security Terms) Data Location (Service Specific Terms) Enabling Customer Compliance Customer Information, Audit and Access Regulator Information, Audit and Access