Austrian FMA - Versicherungsaufsichtsgesetz (VAG)

Google Cloud Mapping

This document is designed to help credit institutions ("**regulated entities**") regulated by the Austrian Financial Markets Authority ("**supervisory authority**") to consider the Versicherungsaufsichtsgesetz or VAG (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: Section 109 (Outsourcing) and Section 321 (Disclosure of Secrets). 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
Section 109 (Outsourcing)			
1.	(1) Insurance and reinsurance undertakings which outsource functions or business activities to service providers remain responsible for meeting all prudential requirements. The outsourcing insurance and reinsurance undertaking shall ensure that:		
2.	1. the service provider cooperates with the FMA;	Google will fully cooperate with supervisory authorities exercising their audit, information and access rights.	Enabling Customer Compliance
3.	2. the undertakings themselves, their statutory auditors and the FMA have effective access to data related to the outsourced functions or business activities;	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. 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
4.	3. the FMA has effective access to the business premises of the service provider; and	Google grants audit, access and information rights to supervisory authorities. This includes access to Google's premises used to provide the Services to conduct an on-site audit.	Regulator Information, Audit and Access
5.	4. the service provider fulfils the conditions of Article 28 (1) of Regulation (EU) 2016/679 and complies with the provisions of Article 28 (3) of Regulation (EU) 2016/679.	Google will comply with all data protection regulations applicable to it in the provision of the Services, including the GDPR. In addition, Google makes commitments to protect your data, including regarding security, use, transfer, access and retention, in the Cloud Data Processing Addendum.	Representations and Warranties
6.	(2) Contracts by which critical or important functions or activities are outsourced must be notified to the FMA in a timely manner prior to the outsourcing. They shall require the prior approval of the FMA where the service provider is not an insurance or reinsurance undertaking.	This is a customer consideration.	N/A
7.	(3) Outsourcing of critical or important operational functions or activities shall not be undertaken if it will lead to any of the following:		
8.	1. materially impairing the quality of the system of governance of the insurance or reinsurance undertaking concerned;	This is a customer consideration.	N/A
9.	2. unduly increasing the operational risk;	You decide which services to use, how to use them and for what purpose. Therefore you stay in control of the relevant activities and can configure the service to avoid undue operational risk.	N/A
10.	3. impairing the ability of the FMA to monitor the compliance of the outsourcing insurance or reinsurance undertaking with the provisions applicable to contractual insurance activities;	Google recognizes that using our Services should not impair the supervisory authority's ability to oversee and supervise compliance with applicable laws and regulations. We will provide regulated entities and their supervisory authorities with the assistance they need to review our Services	Enabling Customer Compliance

Austrian FMA - Versicherungsaufsichtsgesetz

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
11.	4. undermining continuous service provision free from defects to policyholders and beneficiaries.	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. • **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). If Google's performance of the Services does not meet the Google Cloud Platform Service Level Agreements regulated entities may claim service credits.	Ongoing Performance Monitoring Services
12.	Where deemed appropriate to avoid occurrence of the cases referred to in nos. 1 to 4 or to avoid otherwise endangering the interests of the policyholders and beneficiaries, approval can be granted subject to conditions.	This is a customer consideration.	N/A
13.	(4) The outsourcing insurance or reinsurance undertaking shall immediately notify the FMA of any substantial subsequent changes related to the functions and activities outsourced pursuant to para. 2. Where the circumstances referred to in paras. 1 and 3 occur after approval has been granted or where these circumstances apply in the case of an outsourcing contract that is not subject to approval, the FMA may call for the contractual relationship to be terminated.	Updates to the Service 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. Significant Developments 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.	Changes to Services Significant Developments

Austrian FMA - Versicherungsaufsichtsgesetz

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		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. Termination requested by supervisory authority Regulated entities can elect to terminate our contract for convenience with advance notice, including if necessary to comply with the law or if directed by the supervisory authority.	Data Incidents (Cloud Data Processing Addendum) Term and Termination
14.	(5) The FMA may call on the outsourcing insurance or reinsurance undertaking to submit all necessary information on the service provider with which the outsourcing contract is to be concluded or has been concluded, particularly the financial statements as well as other appropriate business records.	Financial statements You can review our audited financial statements, annual reports and information about Google's financial condition on Alphabet's Investor Relations page. Information rights Google grants audit, access and information rights to regulated entities and supervisory authorities. Regulated entities may access their data on the services at any time and may provide their supervisory authority with access.	N/A Regulator Information, Audit and Access; Customer Information, Audit and Access
Section 321 (Disclosure of Secrets)			
15.	Whoever as a member of a body, as a trustee, as a responsible actuary, as an employee of an insurance undertaking, a reinsurance undertaking, a small insurance undertaking or a small mutual association, as a self-employed insurance agent, as an inspecting body pursuant to Section 274 para. 2 VAG or as a government commissioner pursuant to Section 284 para. 1 no. 2 VAG discloses or uses situations or circumstances which have only been revealed to them owing to their professional activities, and the confidentiality of which is in the legitimate interest of the affected persons, shall be deemed to be committing an administrative offence and shall be fined up to EUR 60,000 by the FMA, unless the disclosure or use is justified due to content and form by a public or legitimate private interest, or the person concerned expressly agreed to such disclosure or use.	Google will comply with all laws and regulations applicable to it in the provision of the Services. Google commits to only access or use your data to provide the Services ordered by you. In addition, Google makes commitments to protect your data, including regarding security, in the Cloud Data Processing Addendum. 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.	Representations and Warranties Confidentiality; Protection of Customer Data; Data Security; Security Measures (Cloud Data Processing Addendum)

Austrian FMA - Versicherungsaufsichtsgesetz

Google Cloud Mapping

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

Austrian FMA - Versicherungsaufsichtsgesetz

Google Cloud Mapping

#	Framework reference	Google Cloud commentary	Google Cloud Financial Services Contract reference
		• Security best practices • Security use cases	