

# BaFin Cloud Outsourcing Guidance

## Google Workspace Mapping

This document is designed to help financial institutions (“**regulated entities**”) within the scope of the Bundesanstalt für Finanzdienstleistungsaufsicht’s (BaFin) and the Deutsche Bundesbank’s supervisory mandate to consider the [Guidance on Outsourcing to Cloud Service Providers](#) (the “**BaFin Cloud Outsourcing Guidance**”) in the context of Google Workspace and the Google Cloud Financial Services Contract.

We focus on Section V of the BaFin Cloud Outsourcing Guidance: Contractual terms in the case of (material) outsourcing. For each paragraph of Section V, we provide commentary to help you understand how you can address the guidance using the Google Cloud services and the Google Cloud Financial Services Contract.

#	Framework reference	Google Cloud Commentary	Google Cloud Financial Services Contract reference
1.	<b>Scope of performance</b>		
2.	The agreement should include a specification, and if necessary a description, of the service to be performed by the cloud service provider. This should be stipulated in what is referred to as the service level agreement. In this context, the following aspects should be defined:		
3.	<ul style="list-style-type: none"><li>the item to be outsourced and its implementation (e.g. type of service and deployment model, scope of services offered such as computing power or available memory space, availability requirements, response times),</li></ul>	The Google Workspace services are described on our <a href="#">services summary</a> page.	Definitions
4.	<ul style="list-style-type: none"><li>support services</li></ul>	The support services are described on our <a href="#">technical support services guidelines</a> page.	Technical Support
5.	<ul style="list-style-type: none"><li>responsibilities, duties of cooperation and provision (e.g. in the case of updates)</li></ul>	Refer to your Google Cloud Financial Services Contract.	Services
6.	<ul style="list-style-type: none"><li>place of performance (e.g. location of data centres)</li></ul>	<p>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.</p> <ul style="list-style-type: none"><li>Information about the location of Google’s facilities is available on our <a href="#">Data Center Locations</a> page.</li><li>Information about the location of Google’s subprocessors’ facilities is available on our <a href="#">subprocessor</a> page.</li></ul> <p>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:</p> <ul style="list-style-type: none"><li>The same robust security measures apply to all Google facilities, regardless of country / region.</li><li>Google makes the same commitments about all its subprocessors, regardless of country / region.</li></ul>	Data Transfers ( <a href="#">Cloud Data Processing Addendum</a> )  Data Security; Subprocessors ( <a href="#">Cloud Data Processing Addendum</a> )
7.	<ul style="list-style-type: none"><li>commencement and end of outsourcing agreement</li></ul>	Refer to your Google Cloud Financial Services Contract.	Term and Termination
8.	<ul style="list-style-type: none"><li>key ratios for performing ongoing review of service level</li></ul>	The SLAs are available on our <a href="#">Google Workspace Service Level Agreements</a> page.	Services
9.	<ul style="list-style-type: none"><li>indicators for identifying an unacceptable service level</li></ul>	See Row 8	See Row 8
10.	<b>2. Information and audit rights of supervised company</b>		
11.	Information and audit rights as well as control possibilities of the supervised company must not be subject to contractual restrictions. It has to be ensured that the supervised company receives the information it needs to adequately control and monitor the risks associated with the outsourcing.	Google recognizes that using our Services should not impair a regulated entity’s ability to oversee compliance with applicable laws and regulations as well as a regulated entity’s internal policies. We will provide regulated entities with the assistance they need to review our Services.	Enabling Customer Compliance



# BaFin Cloud Outsourcing Guidance

## Google Workspace Mapping

#	BaFin Outsourcing Guidelines	Google Cloud Commentary	Google Cloud Financial Services Contract reference
12.	To safeguard the information and audit rights, the following terms in particular should be contractually agreed:		
13.	<ul style="list-style-type: none"><li>grant of full access to information and data as well as access to the cloud service provider's business premises, including all data centres, equipment, systems, networks used for providing the items outsourced; this includes the related processes and controls,</li></ul>	Google grants information, audit and access rights to regulated entities and their appointees. This includes access to Google's premises used to provide the Services to conduct an on-site audit.	Customer Information, Audit and Access
14.	<ul style="list-style-type: none"><li>the possibility of performing on-site audits of the cloud service provider (and where applicable of the chain-outsourcing company),</li></ul>	See Row 13. In addition, Google recognizes that chain-outsourcing must not reduce the regulated entity's ability to monitor the service. To preserve this, Google will ensure our subcontractors comply with the information, audit and access rights we provide to regulated entities.	Google Subcontractors
15.	<ul style="list-style-type: none"><li>effective possibilities of controlling and auditing the entire outsourcing chain.</li></ul>	See Row 14	See Row 14
16.	<b>No (indirect) restriction of rights</b>		
17.	Effective exercise of the information and audit rights may not be restricted by contract. The German supervisory authorities consider such impermissible restriction of information and auditing rights to exist particularly in the case of contractual agreements granting such rights only subject to certain conditions.	Nothing in our contract is intended to restrict a regulated entity's ability to monitor or audit our services effectively.	Enabling Customer Compliance
18.	This particularly includes:		
19.	<ul style="list-style-type: none"><li>agreeing on incremental information and audit procedures, e.g. the obligation to first rely on the audit reports, certificates or other proof of compliance with recognised standards by the cloud service provider before the supervised company can perform its own auditing activities,</li></ul>	Although we will make a lot of information and tools available to help regulated entities review our Services, our contract does not contain predefined steps before regulated entities can approach Google to exercise their information, audit and access rights. In other words, there is no hierarchy amongst the options for assessing our Services.	Customer Information, Audit and Access
20.	<ul style="list-style-type: none"><li>restricting performance of information and audit rights to submission of audit reports, certificates or other proof of compliance with recognised standards by the cloud service provider,</li></ul>	Google offers regulated entities certifications and audit reports in addition to (and not instead of) information, audit and access rights.	Certifications and Audit Reports; Customer Information, Audit and Access
21.	<ul style="list-style-type: none"><li>linking information access to prior attendance of special training programmes,</li></ul>	Google does not link the regulated entity's access to information to participation in training programs.	Customer Information, Audit and Access
22.	<ul style="list-style-type: none"><li>wording a clause in such a way that performance of an audit is made conditional on its commercial reasonableness,</li></ul>	Google does not make the regulated entity's exercise of information, audit and access rights conditional on commercial reasonableness.	Customer Information, Audit and Access
23.	<ul style="list-style-type: none"><li>limiting the performance of audits in terms of timing and personnel; as a general rule, however, it is acceptable to limit access to customary business hours upon advance notice,</li></ul>	Conducting an audit during business hours with advance notice enables Google to deliver an effective audit. For example, we can ensure the relevant Google experts are available and prepared to make the most of your time. Notice also enables Google to plan the audit so that it	Arrangements



# BaFin Cloud Outsourcing Guidance

## Google Workspace Mapping

#	BaFin Outsourcing Guidelines	Google Cloud Commentary	Google Cloud Financial Services Contract reference
		does not create undue risk to your environment or that of any other Google customer.	
24.	<ul style="list-style-type: none"><li>making reference to exclusive use e.g. of management consoles for exercising information and audit rights of the company,</li></ul>	Google offers regulated entities control and monitoring functionality via the Admin Console in addition to (and not instead of) information, audit and access rights.	Customer Information, Audit and Access
25.	<ul style="list-style-type: none"><li>specifying the procedure as well as the scope by which information and audit rights are exercised by the cloud service provider.</li></ul>	The regulated entity is best placed to decide what audit frequency and scope is right for their organization. Our contract does not limit regulated entities to a fixed number of audits or a pre-defined scope.	Customer Information, Audit and Access
26.	<b>Exemptions</b>		
27.	Depending on the applicable requirements under supervisory law, the supervised companies may claim exemptions to make their own audit activities more efficient. Such exemptions are pooled audits or the use of documentation/certificates based on common standards or of audit reports of recognised third parties or of internal audit reports of the cloud service provider.	This is a customer consideration. Although we will make a lot of information and options available to help regulated entities review our Services, we recognize that the regulated entity is best placed to decide how to make their audit activities more efficient.	N/A
28.	<b>Pooled audits</b>		
29.	Supervised companies subject to compliance with sections 25a, 25b KWG may avail themselves of exemptions in Circular 09/2017 (BA) – Minimum Requirements for Risk Management – (MaRisk). Pursuant to BT 2.1 Item 3 MaRisk, the internal auditing function of the supervised company in the case of material outsourcing may forego own auditing activities provided that the auditing work carried out by the external service provider meets the requirements of AT 4.4 and BT 2 MaRisk. The internal auditing function of the supervised outsourcing company must satisfy itself at regular intervals that these conditions are met. The audit findings concerning the supervised company are to be passed on to the internal auditing function of the supervised outsourcing company.	<p>This is a customer consideration.</p> <p>See Rows 10 to 25 for the information, audit and access rights that Google provides to regulated entities.</p> <p>See Rows 33 to 35 for the certifications and audit reports Google provides to regulated entities.</p>	N/A
30.	In this regard the auditing activity may be performed by the internal audit department of the cloud service provider, the internal audit department of one or more of the supervised outsourcing companies on behalf of the supervised outsourcing companies ("pooled audits"), a third party appointed by the cloud service provider or a third party appointed by the supervised outsourcing companies.	<p>See Rows 10 to 25. Google grants information, audit and access rights to regulated entities and their appointees. This includes the regulated entity's internal audit department or a third party auditor appointed by the regulated entity.</p> <p>See Rows 33 to 35. The certifications and audit reports Google provides to regulated entities are prepared by qualified and independent third party auditors.</p>	<p>Customer Information, Audit and Access</p> <p>Certifications and Audit Reports</p>
31.	For the other supervised companies, it may be permissible in the individual case to exercise certain information and audit rights against the cloud service provider jointly with other supervised companies by way of pooled audit.	Google recognizes the benefits of pooled audits. We would be happy to discuss this with regulated entities.	N/A



# BaFin Cloud Outsourcing Guidance

## Google Workspace Mapping

#	BaFin Outsourcing Guidelines	Google Cloud Commentary	Google Cloud Financial Services Contract reference
32.	If a supervised company avails itself of one of the aforementioned exemptions, this may not result in its information and audit rights being restricted.	Regulated entities always retain the right to conduct an audit. These rights are not impacted if a regulated entity chooses to review audit reports provided by Google or participate in a pooled audit.	Customer Information, Audit and Access
33.	<b>Proof/certificates and audit reports</b>		
34.	The supervised company as a general rule may use documentation/certificates on the basis of common standards (e.g. international security standard ISO/IEC 2700X of the International Organization for Standardization, Cloud Computing Compliance Controls Catalogue (C 5 Catalogue) of the BSI), audit reports of recognised third parties or internal audit reports of the cloud service provider. The supervised company in this regard must take account of the scope, depth of detail, up-to-dateness and suitability of the certifier or auditor of such documentation/certificates and audit reports.	<p>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:</p> <ul style="list-style-type: none"><li>• <a href="#">ISO/IEC 27001:2013</a> (Information Security Management Systems)</li><li>• <a href="#">ISO/IEC 27017:2015</a> (Cloud Security)</li><li>• <a href="#">ISO/IEC 27018:2014</a> (Cloud Privacy)</li><li>• <a href="#">SOC 1 report</a></li><li>• <a href="#">SOC 2 report</a></li><li>• <a href="#">SOC 3 report</a></li></ul> <p>Where requested by German regulated entities, Google will also provide its <a href="#">BSI C5 report</a>.</p> <p>Google is audited at least once a year for each audited framework. Google's audit scope covers Services, infrastructure systems, policies and procedures, common processes and personnel. As part of Google's routine planning, scoping, and readiness activities, recurring key systems and controls, as well as new systems and controls, are reviewed prior to the audit work commencing.</p> <p>Google engages qualified and independent third party auditors for each audited framework. Refer to the relevant certification or audit report for information on the certifying or auditing party.</p>	Certifications and Audit Reports
35.	However, a supervised company must not rely solely on these when exercising its audit activity. Where the internal audit department uses such documentation/certificates in its activity, it should be able to examine the evidence underlying them.	Regulated entities always retain the right to conduct an audit. Google offers regulated entities certifications and audit reports in addition to (and not instead of) audit, access and information rights.	Customer Information, Audit and Access
36.	<b>3. Information and audit rights of supervisory authorities</b>		
37.	<ul style="list-style-type: none"><li>• Information and audit rights as well as control possibilities of the supervisory authorities must not be subject to contractual restrictions. The supervisory authorities must be able to monitor cloud service providers exactly as the applicable law provides for the supervised company. It must be possible for the</li></ul>	Google recognizes that using our Services should not impair the supervisory authority's ability to supervise compliance with applicable laws and regulations. We will provide supervisory authorities with the assistance they need to review our Services.	Enabling Customer Compliance



# BaFin Cloud Outsourcing Guidance

## Google Workspace Mapping

#	BaFin Outsourcing Guidelines	Google Cloud Commentary	Google Cloud Financial Services Contract reference
	supervisory authorities to exercise their information and audit rights as well as control possibilities properly, and without restriction, as regards the item being outsourced; this also applies to those persons whom the supervisory authorities use when performing the audits.		
38.	To safeguard these rights, the following terms in particular should be contractually agreed:		
39.	<ul style="list-style-type: none"><li>obligation of the cloud service provider to cooperate with the supervisory authorities without restriction,</li></ul>	Google will fully cooperate with supervisory authorities and resolution authorities exercising their audit, information and access rights.	Enabling Customer Compliance
40.	<ul style="list-style-type: none"><li>grant of full access to information and data as well as access to the cloud service provider's business premises, including all data centres, equipment, systems, networks used for providing the items outsourced; this includes the processes and controls relating thereto as well as the possibility of performing on-site audits of the cloud service provider (and where applicable of the chain-outsourcing company),</li></ul>	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
41.	<ul style="list-style-type: none"><li>effective possibilities of controlling and auditing the entire outsourcing chain</li></ul>	Google recognizes that chain-outsourcing must not reduce the supervisory authority's ability to supervise the regulated entity. To preserve this, Google will ensure our subcontractors comply with the information, access and audit rights we provide to supervisory authorities.	Google Subcontractors
42.	No (indirect) restriction of rights)		
	Such impermissible restriction of information and auditing rights as well as control possibilities of the German supervisory authorities is deemed to exist particularly in the case of provisions granting such rights only on certain conditions. We refer to the above statements on the restriction of the rights of the supervised companies to avoid repetition.	Nothing in our contract is intended to restrict the supervisory authority's ability to monitor and audit our services effectively. See Rows 16 to 25.	Enabling Customer Compliance; Regulator Information, Audit and Access
43.	<b>4. Rights to issue instructions</b>		
44.	Rights of the supervised companies to issue instructions are to be agreed. The rights to issue instructions are to ensure that all required instructions needed to perform the agreed service can be issued, i.e. the possibility of influencing and controlling the outsourced item is required. The technical implementation may be organised individually based on the company's specific circumstances.	Regulated entities have the right to issue instructions to Google. To do this, regulated entities can use the the following functionality of the Services: <ul style="list-style-type: none"><li><a href="#">Admin Console</a>: A web-based graphical user interface that customers can use to manage their Google Workspace resources.</li></ul>	Instructions
45.	If the supervised company uses proof/certifications or audit reports (cf. V.2), it should also have the possibility of influencing the scope of proof/certifications or audit reports so that	To ensure that they remain an effective tool, if a key system or control for a Service is not covered by Google's certifications or audit reports for that service, regulated entities can request an expansion of the scope.	Certifications and Audit Reports



# BaFin Cloud Outsourcing Guidance

## Google Workspace Mapping

#	BaFin Outsourcing Guidelines	Google Cloud Commentary	Google Cloud Financial Services Contract reference
	it can be expanded to include relevant systems and controls. There should be a reasonable proportion in how many and how often such instructions are issued.		
46.	Moreover, the supervised company should be authorised at all times to issue instructions to the cloud service provider for correction, deletion and blocking of data and the cloud service provider should be allowed to collect, process and use the data only in the context of the instructions issued by the supervised company. This should also cover the possibility of issuing an instruction at any time to have the data processed by the cloud service provider transferred back to the supervised company promptly and without restriction.	<p><u>Correction, erasure and blocking</u></p> <p>Google provides functionality to enable customers to access, rectify, and restrict processing of their data as well as retrieve or delete data.</p> <p><u>Processing in accordance with instructions</u></p> <p>Google will comply with the customer's instructions for the processing of data.</p>	<p>Access; Rectification; Restricted Processing; Portability (<a href="#">Cloud Data Processing Addendum</a>)</p> <p>Data Deletion (<a href="#">Cloud Data Processing Addendum</a>)</p> <p>Scope of Processing; Customer's Instructions (<a href="#">Cloud Data Processing Addendum</a>)</p>
47.	If the explicit agreement on the rights of the supervised company to issue instructions can be waived, the service to be provided by the outsourcing company is to be specified with sufficient clarity in the outsourcing agreement.	See Row 44.	See Row 44.
48.	<b>5. Data security/protection (reference to location of data storage)</b>		
49.	Provisions ensuring compliance with data protection regulations and other security requirements are to be agreed.	<p><u>Data protection</u></p> <p>Google will comply with all European and national data protection regulations applicable to it in the provision of the Services. This is addressed in the <a href="#">Cloud Data Processing Addendum</a>.</p> <p><u>Security</u></p> <p>This is addressed in the <a href="#">Cloud Data Processing Addendum</a>. The security of a cloud service consists of two key elements:</p> <p>(1) <u>Security of Google's infrastructure</u></p> <p>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.</p>	<p>Representations and Warranties</p> <p>Data Security (<a href="#">Cloud Data Processing Addendum</a>)</p>





# BaFin Cloud Outsourcing Guidance

## Google Workspace Mapping

#	BaFin Outsourcing Guidelines	Google Cloud Commentary	Google Cloud Financial Services Contract reference
		<p>More information is available at:</p> <ul style="list-style-type: none"><li>• Our <a href="#">infrastructure security</a> page</li><li>• Our <a href="#">security whitepaper</a></li><li>• Our <a href="#">cloud-native security whitepaper</a></li><li>• Our <a href="#">infrastructure security design overview</a> page</li><li>• Our <a href="#">security resources</a> page</li></ul> <p>In addition, you can review Google's <a href="#">SOC 2 report</a>. See Row 34.</p> <p>(2) <u>Security of your data and applications in the cloud</u></p> <p>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.</p> <p>(a) <u>Security by default</u></p> <p>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:</p> <ul style="list-style-type: none"><li>• <b>Encryption at rest.</b> Google encrypts certain data while it is stored at rest on a disk (including solid-state drives) or backup media. Even if an attacker or someone with physical access obtains the storage equipment containing your data, they won't be able to read it because they don't have the necessary encryption keys.</li><li>• <b>Encryption in transit.</b> Google encrypts all data while it is "in transit"—traveling over the Internet and across the Google network between data centers. Should an attacker intercept such transmissions, they will only be able to capture encrypted data, at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google.</li></ul> <p>(b) <u>Security products</u></p> <p>In addition to the other tools and practices available to you outside Google, you can choose to</p>	



# BaFin Cloud Outsourcing Guidance

## Google Workspace Mapping

#	BaFin Outsourcing Guidelines	Google Cloud Commentary	Google Cloud Financial Services Contract reference
		<p>use tools provided by Google to enhance and monitor the security of your data. Information on Google's security products is available on our <a href="#">Cloud Security Products</a> page.</p> <p>(c) <a href="#">Security resources</a></p> <p>Google also publishes guidance on:</p> <ul style="list-style-type: none"><li>• Security best <a href="#">practices</a></li><li>• Security use <a href="#">cases</a></li></ul>	
50.	The location of data storage must be known to the supervised company. This should include the specific location of the data centres. As a general rule, giving the name of the location (e.g. the town or city) will suffice for this purpose. However, if the supervised company should need the precise address of the data centre based on considerations of risk management, the cloud service provider should provide it.	<p>See Row 6 on the location of Google's facilities</p> <p>Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s).</p> <p>You can also choose to use tools provided by Google to enforce data location requirements. For more information, see our <a href="#">whitepaper</a>.</p>	Data Regions ( <a href="#">Service Specific Terms</a> )
51.	Moreover, redundancy of the data and systems should be ensured so that in the event of a failure of one data centre it is ensured that the services are maintained.	<p>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.</p> <p>Information on the reliability of the Services is available on our <a href="#">Google Cloud Help</a> page.</p>	Business Continuity and Disaster Recovery
52.	The security of the data and systems is also to be ensured within the outsourcing chain.	Google requires our subcontractors to meet the same high standards that we do. In particular, Google requires our subcontractors to comply with our contract with you.	Google Subcontractors
53.	The supervised company must have the possibility of quickly accessing at all times its data stored with the cloud service provider and of re-transferring the same if required. In this regard it has to be ensured that the selected form of re-transfer does not restrict or exclude the use of the data. For that reason, platform-independent standard data formats should be agreed. Compatibility of the different system must be taken into account.	Google will enable you to access and export your data throughout the duration of our contract and the transition term. More information is available on our <a href="#">Google Account help</a> page. In addition, <a href="#">Data Export</a> is a feature that makes it easy to export and download a copy of your data securely from our Services.	Data Export ( <a href="#">Cloud Data Processing Addendum</a> )
54.	<b>6. Termination provisions</b>		
55.	Termination rights and adequate termination notice periods are to be agreed. In particular, a special termination right, providing for termination for good cause if the supervisory authority calls for the agreement to be ended, should be agreed.	Regulated entities can elect to terminate our contract for convenience, including if necessary to comply with law or if directed by the supervisory authority.	Termination for Convenience





# BaFin Cloud Outsourcing Guidance

## Google Workspace Mapping

#	BaFin Outsourcing Guidelines	Google Cloud Commentary	Google Cloud Financial Services Contract reference
56.	It has to be ensured that in the event of termination the items outsourced to the cloud service provider continue to be provided until such time that the outsourced item has been completely transferred to another cloud service provider or to the supervised company. In this regard it has to be guaranteed in particular that the cloud service provider will reasonably assist the supervised company in transferring the outsourced items to another cloud service provider or directly to the supervised company.	<p>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</p> <p>Our Services enable you to transfer your data independently. You do not need Google's permission to do this. See Row 53 for details. However, if a regulated entity would like support, upon request, Google will provide advisory and implementation services to assist in migrating workloads or otherwise transitioning use of the Services.</p>	<p>Transition Term</p> <p>Transition Assistance</p>
57.	The type, form and quality of transfer of the outsourced item and the data should be defined. If data formats are adapted to the individual needs of the supervised company, the cloud service provider should deliver a documentation of such adaptations on termination.	See Row 53	See Row 53
58.	It should be agreed that after re-transfer of the data to the supervised company its data have been completely and irrevocably deleted on the side of the cloud service provider.	On termination of the contractual relationship, Google will comply with the regulated entity's instruction to delete Customer Data from Google's systems.	Data Deletion ( <a href="#">Cloud Data Processing Addendum</a> )
59.	To ensure that the outsourced areas are maintained in the event of the planned or unplanned termination of the agreement, the supervised company must have an exit strategy and review its feasibility.	This is a customer consideration. See Row 56 for the post-termination support that Google provides to regulated entities.	N/A
72.	<b>7. Chain Outsourcing</b>		
73.	Provisions on the possibility and the modalities of chain-outsourcing ensuring that the requirements of supervisory law continue to be met are to be agreed. Restrictions resulting, e.g., in only the most substantially similar obligations being assumed are not permissible. It must be ensured in particular that the information and audit rights as well as controlling possibilities of the supervised outsourcing company as well as of the supervisory authorities also apply to subcontractors in the case of chain-outsourcing.	<p>To enable regulated entities to retain oversight of any sub-outsourcing and provide choices about the services regulated entities use, Google will:</p> <ul style="list-style-type: none"><li>• provide information about our subcontractors;</li><li>• provide advance notice of changes to our subcontractors; and</li><li>• give regulated entities the ability to terminate if they have concerns about a new subcontractor.</li></ul> <p>Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you.</p>	Google Subcontractors



# BaFin Cloud Outsourcing Guidance

## Google Workspace Mapping

#	BaFin Outsourcing Guidelines	Google Cloud Commentary	Google Cloud Financial Services Contract reference
		In particular, we recognize that sub-outsourcing must not reduce the regulated entity's ability to oversee the service or the supervisory authority's ability to supervise the regulated entities. To preserve this, Google will ensure our subcontractors comply with the information, audit and access rights we provide to regulated entities and supervisory authorities.	
74.	With a view to chain-outsourcing, reservations of consent of the outsourcing company or specific conditions to be met in order for chain-outsourcing to be possible should be provided for in the outsourcing agreement. It should be defined which outsourced items and/or portions thereof may be chain-outsourced and which ones may not.	<p>Google recognizes that regulated entities need to consider the risks associated with sub-outsourcing. We also want to provide you and all our customers with the most reliable, robust and resilient service that we can. In some cases there may be clear benefits to working with other trusted organizations e.g. to provide 24/7 support.</p> <p>Although Google will provide you with information about the organizations that we work with, we cannot agree that we will never sub-outsource. Given the one-to-many nature of our service, if we agreed with one customer that we would not sub-outsource, we would potentially be denying all our customers the benefit motivating the sub-outsourcing.</p> <p>To ensure regulated entities retain oversight of any sub-outsourcing, Google will comply with clear conditions designed to provide transparency and choice. See Row 73.</p>	Google Subcontractors
75.	The supervised company should be informed in advance of chain-outsourcing of the outsourced items and/or portions thereof in text form. The subcontractors and the items and/or portions thereof chain-outsourced to them should be known to the supervised company.	You need enough time from being informed of a subcontractor change to perform a meaningful risk assessment before the change comes into effect. To ensure you have the time you need, Google provides advance notice before we engage a new subcontractor or change the function of an existing subcontractor.	Google Subcontractors
76.	In the event of a new chain-outsourcing, it has to be kept in mind that this may have impacts on the risk situation of the outsourcing and thus on the outsourcing company. Accordingly, the risk analysis should at least be reviewed or repeated in the event of a new chain outsourcing. This also applies where material defects as well as material changes in the cloud service provided by subcontractors become known.	This is a customer consideration.	N/A
77.	The company should review and monitor the performance of the entire service on an ongoing basis, regardless of whether the cloud service is provided by the cloud service provider or its subcontractors.	<p>You can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services.</p> <p>For example:</p> <ul style="list-style-type: none"><li>• The <a href="#">Status Dashboard</a> provides status information on the Services.</li></ul>	Ongoing Performance Monitoring



# BaFin Cloud Outsourcing Guidance

## Google Workspace Mapping

#	BaFin Outsourcing Guidelines	Google Cloud Commentary	Google Cloud Financial Services Contract reference
		<ul style="list-style-type: none"><li><a href="#">Admin Console Reports</a> allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more.</li><li><a href="#">Access Transparency</a> 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).</li></ul>	
78.	<b>8. Information duties</b>		
79.	Provisions are to be agreed ensuring that the cloud service provider informs the supervised company about developments that might adversely affect the orderly performance of the outsourced items. That includes things like reporting any disruptions in providing the cloud service. This is to ensure that the company can adequately monitor the outsourced item.	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 <a href="#">Status Dashboard</a> .  See Row 77 on how you can monitor Google's performance of the Services.	Significant Developments
80.	The cloud provider is to inform the supervised company without delay about any circumstances that might pose a risk to the security of the supervised company's data to be processed by the cloud service provider, e.g. as a result of acts by third parties (e.g. attachment or confiscation), insolvency or composition proceedings, or other events.	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 <a href="#">Data incident response whitepaper</a> .	Data Incidents ( <a href="#">Cloud Data Processing Addendum</a> )
81	It should be ensured that the supervised company is adequately informed by the cloud service provider in advance in the event of relevant changes in the cloud service to be provided by the cloud service provider. Service descriptions and any changes to them should be provided and/or notified to the supervised company in text form. It should be ensured that the supervised company is adequately informed, to the extent permitted by law, where any requests/demands for surrender of data of the supervised company are made by third parties.	<u>Service changes</u>  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 performance 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.  <u>Lawful access</u>	Changes to Services          Confidentiality



# BaFin Cloud Outsourcing Guidance

## Google Workspace Mapping

#	BaFin Outsourcing Guidelines	Google Cloud Commentary	Google Cloud Financial Services Contract reference
		<p>Google understands that this is important and is committed to maintaining trust with customers by being transparent about how we respond to government requests.</p> <p>If Google receives a government request, Google will:</p> <ul style="list-style-type: none"><li>• attempt to redirect the request to the customer</li><li>• notify the customer prior to disclosure unless prohibited by law</li><li>• comply with the customer requests to oppose disclosure</li><li>• only disclose if strictly necessary to comply with legal process</li></ul> <p>More information about Google's practices around government requests for data is available in our <a href="#">Government Requests for Cloud Customer Data</a> whitepaper.</p> <p>To provide even more transparency, Google reports the government requests we receive for enterprise Cloud customers in our <a href="#">Enterprise Cloud Transparency Report</a>.</p>	
82.	<b>9. Notice of applicable law</b>		
83.	Where a choice of law clause is agreed and German law is not agreed as the governing law, the law of a country from the European Union or the European Economic Area should at any event be agreed as the law governing the agreement.	Refer to your Google Cloud Financial Services Contract. Google offers EU / EEA governing law for the contract.	Governing Law