EIOPA Guidelines on Outsourcing to Cloud Service Providers

Google Workspace Mapping

This document is designed to help insurance and re-insurance undertakings within the scope of the European Insurance and Occupational Pensions Authority's mandate ("**undertakings**") to consider the Guidelines on Outsourcing to Cloud Service Providers in the context of Google Workspace and the Google Cloud Financial Services Contract.

We focus on Guidelines 10 to 15 of the EIOPA Guidelines on Outsourcing to Cloud Service Providers. For each paragraph of those Guidelines, we provide commentary to help you understand how you can address them using the Google Workspace services and the Google Cloud Financial Services Contract.

If you have an existing Google Cloud contract and would like to understand how this document applies to your contract, please contact your Google Cloud account representative.

#	**EIOPA Guidelines on Outsourcing to Cloud Service Providers**	**Google Cloud Commentary**	**Google Cloud Financial Services Contract Reference**
1.	**10 Contractual requirements**		
2	36. The respective rights and obligations of the undertaking and of the cloud service provider should be clearly allocated and set out in a written agreement.	The rights and obligations of the parties are set out in the Google Cloud Financial Services Contract.	N/A
3	37. Without prejudice to the requirements defined in Article 274 of the Delegated Regulation, in case of outsourcing of critical or important operational functions or activities to a cloud service provider, the written agreement between the undertaking and the cloud service provider should set out:		
4	a. a clear description of the outsourced function to be provided (cloud services, including the type of support services);	The Google Workspace services are described on our services summary page. The support services are described on our Google Workspace technical support services guidelines page.	Definitions Technical Support
5	b. the start date and end date, where applicable, of the agreement and the notice periods for the cloud service provider and for the undertaking;	Refer to your Google Cloud Financial Services Contract.	Term and Termination
6	c. the court jurisdiction and the governing law of the agreement;	Refer to your Google Cloud Financial Services Contract.	Governing Law
7	d. the parties' financial obligations;	Refer to your Google Cloud Financial Services Contract.	Payment Terms
8	e. whether the sub-outsourcing of a critical or important operational function or activity (or material parts thereof) is permitted, and, if so, the conditions to which the significant sub-outsourcing is subject to (see Guideline 13);	Refer to the comments on Guideline 13 at rows 52 to 58.	Refer to rows 52 to 58.
9	f. the location(s) (i.e. regions or countries) where relevant data will be stored and processed (location of data centres), and the conditions to be met, including a requirement to notify the undertaking if the service provider proposes to change the location(s);	Locations 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 is available on our Data	Data Transfers (Cloud Data Processing Addendum)

EIOPA Guidelines on Outsourcing to Cloud Service Providers

Google Workspace Mapping

		Center Locations page. • Information about the location of Google's subprocessors' facilities is available on our subprocessor 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. Options 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). More information is available on our Data Regions page.	Data Security; Subprocessors (Cloud Data Processing Addendum) Data Location (Service Specific Terms) Data Transfers (Cloud Data Processing Addendum)
10	g. provisions regarding the accessibility, availability, integrity, confidentiality, privacy and safety of relevant data, taking into account the specifications of Guideline 12;	Refer to the comments on Guideline 12 at rows 39 to 51.	Refer to rows 39 to 51.
11	h. the right for the undertaking to monitor the cloud service provider's performance on a regular basis;	Monitoring 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. • **Admin Console Reports** allow you to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. • **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).	Ongoing Performance Monitoring

EIOPA Guidelines on Outsourcing to Cloud Service Providers

Google Workspace Mapping

12	i. the agreed service levels which should include precise quantitative and qualitative performance targets in order to allow for timely monitoring so that appropriate corrective actions can be taken without undue delay if agreed service levels are not met;	The SLAs are available on our Google Workspace Service Level Agreement page.	Services
13	j. the reporting obligations of the cloud service provider to the undertaking, including, as appropriate, the obligations to submit reports relevant for the undertaking's security function and key functions, such as reports of the internal audit function of the cloud service provider;	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 Google Workspace Status Dashboard. 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 (Cloud Data Processing Addendum)
14	k. whether the cloud service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;	Google will maintain insurance cover against a number of identified risks.	Insurance
15	l. the requirements to implement and test business contingency plans;	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. More information on the reliability of the Services is available on our Google Cloud Help page.	Business Continuity and Disaster Recovery
16	m. the requirement for the cloud service provider to grant the undertaking, its supervisory authorities and any other person appointed by the undertaking or the supervisory authorities, the following:		
17	i. full access to all relevant business premises (head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the cloud service provider's external auditors ("access rights");	Google grants audit, access and information rights to undertakings, supervisory authorities (including resolution authorities) and both their appointees.	Regulator Information, Audit and Access; Customer Information, Audit and Access
18	ii. unrestricted rights of inspection and auditing related to the cloud outsourcing arrangement ("audit rights"), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements;	Google grants audit, access and information rights to undertakings, supervisory authorities (including resolution authorities) and both their appointees.	Regulator Information, Audit and Access; Customer Information, Audit and Access
19	n. provisions to ensure that the data owned by the undertaking can be promptly recovered by the undertaking in case of the insolvency, resolution or discontinuation of business operations of the cloud service provider.	You retain all intellectual property rights in your data. Google will enable you to access and export your data throughout the duration of our contract. Refer to row 68. Neither of these commitments are disapplied on Google's insolvency. Nor does Google have the right to terminate for Google's own insolvency - although you can elect to	Intellectual Property Data Export (Cloud Data Processing Addendum) Term and Termination

EIOPA Guidelines on Outsourcing to Cloud Service Providers

Google Workspace Mapping

		terminate. In the unlikely event of Google's insolvency, you can refer to these commitments when dealing with the appointed insolvency practitioner.	
20	**11 Access and audit rights**		
21	38. The cloud outsourcing agreement should not limit the undertaking's effective exercise of access and audit rights as well as control options on cloud services in order to fulfil its regulatory obligations.	Nothing in our contract is intended to limit or impede an undertaking's or the supervisory authority's ability to audit our services effectively. In particular, although we will make a lot of information and tools available to help undertakings review our Services, our contract does not contain pre-defined steps before undertakings or supervisory authorities can approach Google to exercise their audit, access and information rights. In other words, there is no hierarchy amongst the options for assessing our Services.	Enabling Customer Compliance
22	39. The undertaking should exercise its access and audit rights, determine the audit frequency and the areas and services to be audited on a risk-based approach, according to Section 8 of EIOPA Guidelines on System of Governance.	The undertaking is best placed to decide what audit frequency and scope is right for their organization. Our contract does not limit undertakings to a fixed number of audits or a pre-defined scope.	Customer Information, Audit and Access
23	40. In determining the frequency and the scope of its exercise of access or audit rights, the undertaking should consider whether the cloud outsourcing is related to a critical or important operational function or activity, the nature and extent of risk and impact on the undertaking from the cloud outsourcing arrangements.	This is a customer consideration.	N/A
24	41. If the exercise of its access or audit rights, or the use of certain audit techniques creates a risk for the environment of the cloud service provider and/or another cloud service provider's client (for example, the impact on service levels, availability of data, confidentiality aspects), the undertaking and the cloud service provider should agree on alternative ways to provide a similar level of assurance and service to the undertaking (for example, the inclusion of specific controls to be tested in a specific report/certification produced by the cloud service provider).	It is extremely important to Google that what we do with one customer should not put any other customers at risk. This applies when you perform an audit. It also applies when any other customer performs an audit. When an undertaking performs an audit we will work with them to minimize the disruption to our other customers. Just as we will work with another auditing customer to minimize the disruption to the undertaking. In particular, we will be careful to comply with our security commitments at all times.	Arrangements
25	42. Without prejudice to their final responsibility regarding the activities performed by their cloud service providers, in order to use audit resources more efficiently and decrease the organisational burden on the cloud service provider and its customers, undertakings may use:		
26	a. third-party certifications and third-party or internal audit reports made available by the cloud service provider;	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)	Certifications and Audit Reports

EIOPA Guidelines on Outsourcing to Cloud Service Providers

Google Workspace Mapping

		• ISO/IEC 27018:2014 (Cloud Privacy) • SOC 1 • SOC 2 • SOC 3	
27	b. pooled audits (i.e. performed jointly with other clients of the same cloud service provider), or pooled audits performed by a third-party appointed by them.	Google recognizes the benefits of pooled audits. We would be happy to discuss this with undertakings.	N/A
28	43. In case of cloud outsourcing of critical or important operational functions or activities, undertakings should make use of the method referred to in paragraph 42(a) only if they:		
29	a. ensure that the scope of the certification or the audit report covers the systems (for example, processes, applications, infrastructure, data centres, etc.) and the controls identified by the undertaking and assesses the compliance with relevant regulatory requirements;	Refer to row 26. Google's audit scope covers in-scope Services, infrastructure systems, policies and procedures, common processes and personnel. Google is audited on our security and privacy controls covering the relevant certifications and audit reports for the audit scope.	Certifications and Audit Reports
30	b. thoroughly assess the content of new certifications or audit reports on an regular basis and verify that the certifications or reports are not obsolete;	Refer to row 26. You can review Google's current certifications and audit reports at any time. • Google's **ISO certifications** are available on our Compliance Resource Center. • Google's **SOC reports** and **PCI Attestation of Compliance (AOC)** are available to customers under NDA and can be requested from your Google Workspace account representative.	Certifications and Audit Reports
31	c. ensure that key systems and controls are covered in future versions of the certification or audit report;	Refer to row 26. 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.	Certifications and Audit Reports
32	d. are satisfied with the aptitude of the certifying or auditing party (for example, with regard to rotation of the certifying or auditing company, qualifications, expertise, re-performance/verification of the evidence in the underlying audit file);	Refer to row 26. Google engages certified 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.	Certifications and Audit Reports
33	e. are satisfied that certifications are issued and that the audits are performed according to appropriate standards and include a test of the operational effectiveness of the key controls in place;	Refer to row 26. Audits include testing of operational effectiveness of key controls in place.	Certifications and Audit Reports

EIOPA Guidelines on Outsourcing to Cloud Service Providers

Google Workspace Mapping

34	f. have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective;	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, undertakings can request an expansion of the scope.	Certifications and Audit Reports
35	g. retain the contractual right to perform individual on-site audits at their discretion with regard to the cloud outsourcing of critical or important operational functions or activities; such right should be exercised in case of specific needs not possible through other types of interactions with the cloud service provider.	Undertakings always retain the right to conduct an audit. The contract does not contain pre-defined steps before undertakings can approach Google to exercise their audit, access and information rights. In other words, there is no hierarchy amongst the options for assessing our Services.	Customer Information, Audit and Access
36	44. For outsourcing to cloud service providers of critical or important operational functions, the undertaking should assess whether third-party certifications and reports as referred to in paragraph 42(a) are adequate and sufficient to comply with its regulatory obligations and, on a risk based approach, should not rely solely on these reports and certificates over time.	This is a customer consideration.	N/A
37	45. Before a planned on-site visit, the party to exercise its right of access (undertaking, auditor or third-party acting on behalf of the undertaking(s)) should provide prior notice in a reasonable time period, unless an early prior notification has not been possible due to an emergency or crisis situation. Such notice should include the location and purpose of the visit and the personnel that will participate in the visit.	Reasonable 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 does not create undue risk to your environment or that of any other Google customer. Google recognizes that in some cases extended notice is not possible. In these cases we will work with the auditing party to address their needs.	Arrangements
38	46. Considering that cloud solutions have a high level of technical complexity, the undertaking should verify that the staff performing the audit – being its internal auditors or the pool of auditors acting on its behalf, or the cloud service provider's appointed auditors – or, as appropriate, the staff reviewing the third-party certification or service provider's audit reports have acquired the appropriate skills and knowledge to perform the relevant audits and/or assessments.	This is a customer consideration.	N/A
39	**12 Security of data and systems**		
40	47. The undertaking should ensure that cloud service providers comply with European and national regulations as well as appropriate ICT security standards.	European and national regulations Google will comply with all European and national laws and regulations applicable to it in the provision of the Services. Appropriate ICT security standards Refer to row 26.	Representations and Warranties Refer to row 26.

EIOPA Guidelines on Outsourcing to Cloud Service Providers

Google Workspace Mapping

41	48. In case of outsourcing of critical or important operational functions or activities to cloud service providers, the undertaking should additionally define specific information security requirements in the outsourcing agreement and monitor compliance with these requirements on a regular basis.	The security of a cloud service consists of two key elements: 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. This is described in the Cloud Data Processing Addendum. 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. Refer to row 26. 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 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.	Data Security; Security Measures (Cloud Data Processing Addendum)

EIOPA Guidelines on Outsourcing to Cloud Service Providers

Google Workspace Mapping

		• **Encryption in transit.** 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. See our Google Workspace encryption whitepaper for more information. (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. Here are some examples: • **Cloud Identity** is a unified identity, access, app, and endpoint management (IAM/EMM) platform that helps IT and security teams maximize end-user efficiency and protect your organization's data. • **Security Center** provides actionable security insights for Google Workspace to help protect your organization. • **Alert Center** providers real-time actionable alerts and security insights about activity in your Google Workspace domain. (c) Security resources Google also publishes guidance on: • Security best practices • Security use cases	
42	49. For the purposes of paragraph 48, in case of outsourcing of critical or important operational functions or activities to cloud service providers, the undertaking, applying a risk based approach, and taking into account its responsibilities and the ones of the cloud service provider, should:		

EIOPA Guidelines on Outsourcing to Cloud Service Providers

Google Workspace Mapping

43	a. agree on clear roles and responsibilities between the cloud service provider and the undertaking in relation to the operational functions or activities affected by the cloud outsourcing, which should be clearly split;	Refer to row 41 for more information on Google and the customer's roles and responsibilities in relation to operational functions or activities regarding the security of data and systems.	Refer to row 41.
44	b. define and decide on an appropriate level of protection of confidential data, continuity of activities outsourced, integrity and traceability of data and systems in the context of the intended cloud outsourcing;	Refer to rows 11 and 41 for more information on protection of data and traceability of data and systems. Refer to row 15 for more information on continuity.	Refer to rows 11, 15 and 41.
45	c. consider specific measures, where necessary, for data in transit, data in memory and data at rest, for example, the use of encryption technologies in combination with an appropriate keys management;	Refer to row 41 for more information about encryption at rest and encryption in transit. More information about encryption is available on our Google Cloud Help page.	
46	d. consider the mechanisms of integration of the cloud services with the systems of the undertakings, for example, the Application Programming Interfaces and a sound user and access management process;	There are a number of ways to integrate our services with your systems and to perform effective access management. **Integration** • Google Workspace Marketplace API allows you to access a repository of Google Workspace APIs in a centralized location for easy integration. • Google Workspace also enables you to integrate with reliable third-party business solutions. More information is available on our Partner Integration page. **Access management** • Google Admin Console allows you to add users to your account, turn on the services you want them to use, grant people administrator access, and otherwise manage Google services for your organization. • Cloud Identity is a unified identity, access, app, and endpoint management (IAM/EMM) platform that helps IT and security teams maximize end-user efficiency and protect your organization's data. • Security Center provides actionable security insights for Google Workspace to help protect your organization.	N/A

EIOPA Guidelines on Outsourcing to Cloud Service Providers

Google Workspace Mapping

		• More information on customizing access to Google Workspace services using access groups is available on our Google Workspace Admin Help page.	
47	e. contractually ensure that network traffic availability and expected capacity meet strong continuity requirements, where applicable and feasible;	The SLAs contain Google's commitments regarding availability of the Services. The SLAs are available on our Google Workspace Service Level Agreement page. Google's IP data network allows us to deliver highly available and low latency services across the globe. In the event of network failure, data is automatically shifted from one facility to another so that Google Workspace customers can continue working in most cases without interruption. Customers with global workforces can collaborate on documents, video conferencing and more without additional configuration or expense. Global teams share a highly performant and low latency experience as they work together on a single global network.	Services
48	f. define and decide on proper continuity requirements ensuring adequate levels at each level of the technological chain, where applicable;	Refer to row 15 for more information on continuity.	Refer to row 15.
49	g. have a sound and well documented incident management process including the respective responsibilities, for example, by the definition of a cooperation model in case of actual or suspected incidents occur;	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 whitepaper.	Data Incidents (Cloud Data Processing Addendum
50	h. adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) and information security considerations;	This is a customer consideration. Refer to row 9 for more information on data location.	N/A
51	i. monitor the fulfilment of the requirements relating to the effectiveness and efficiency of control mechanisms implemented by the cloud service provider that would mitigate the risks related to the provided services.	This is a customer consideration. Refer to: • row 11 for more information on how you can monitor Google's performance of the Services; • row 41 for more information on how you can monitor the security of your data; and • the comments on Guideline 11 at rows 21 to 38.	N/A
52	**13 Sub-outsourcing of critical or important operational functions or activities**		
53	50. If sub-outsourcing of critical or important operational functions (or a part thereof) is permitted, the cloud outsourcing agreement between the undertaking and the cloud service provider should:		

EIOPA Guidelines on Outsourcing to Cloud Service Providers

Google Workspace Mapping

54	a. specify any types of activities that are excluded from potential sub-outsourcing;	Google recognizes that undertakings 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. 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. To ensure undertakings retain oversight of any sub-outsourcing, Google will comply with clear conditions designed to provide transparency and choice. Refer to row 55.	Subcontracting
55	b. indicate the conditions to be complied with in case of sub-outsourcing (for example, that the sub-outsourcer will also fully comply with the relevant obligations of the cloud service provider). These obligations include the audit and access rights and the security of data and systems;	To enable undertakings to retain oversight of any sub-outsourcing and provide choices about the services undertakings use, Google will: • provide information about our subcontractors; • provide advance notice of changes to our subcontractors; and • give undertakings the ability to terminate if they have concerns about a new subcontractor. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you (including the audit and access rights, and security requirements).	Google Subcontractors
56	c. indicate that the cloud service provider retains full accountability and oversight for the services sub-outsourced;	Refer to row 55.	Refer to row 55.
57	d. include an obligation for the cloud service provider to inform the undertaking of any planned significant changes to the sub-contractors or the sub-outsourced services that might affect the ability of the service provider to meet its obligations under the cloud outsourcing agreement. The notification period for those changes should allow the undertaking, at least, to carry out a risk assessment of the effects of the proposed changes before the actual change in the sub-outsourcers or the sub-outsourced services comes into effect;	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 commits to give you at least 180 days' advance notice before we engage a new subcontractor or change the function of an existing subcontractor.	Google Subcontractors
58	e. ensure, in cases where a cloud service provider plans changes to suboutsourcer or sub-outsourced services that would have an adverse effect on the risk assessment of the agreed services, that the undertaking has the right to object to such changes and/or the right to terminate and exit the contract.	Undertakings should have a choice about the parties who provide services to them. To ensure this, undertakings have the choice to terminate our contract if they think that a subcontractor change materially increases their risk or if they do not receive the agreed notice.	Google Subcontractors

EIOPA Guidelines on Outsourcing to Cloud Service Providers

Google Workspace Mapping

59	**14 Monitoring and oversight of cloud outsourcing arrangements**		
60	51. The undertaking should monitor, on a regular basis, the performance of activities, the security measures and the adherence to agreed service level by their cloud service providers on a risk based approach. The main focus should be on the cloud outsourcing of critical and important operational functions.	This is a customer consideration. Refer to row 11 for more information on how you can monitor Google's performance of the Services. Refer to row 41 for more information on how you can monitor the security of your data.	N/A
61	52. In order to do so, the undertaking should set up monitoring and oversight mechanisms, which should take into account, where feasible and appropriate, the presence of sub-outsourcing of critical or important operational functions or a part thereof.	Refer to row 60. Refer to the comments on Guideline 13 at rows 52 to 58.	Refer to row 60.
62	53. The AMSB should be periodically updated on the risks identified in the cloud outsourcing of critical or important operational functions or activities.	This is a customer consideration.	N/A
63	54. In order to ensure the adequate monitoring and oversight of their cloud outsourcing arrangements, undertakings should employ enough resources with adequate skills and knowledge to monitor the services outsourced to the cloud. The undertaking's personnel in charge of these activities should have both ICT and business knowledge as deemed necessary	This is a customer consideration.	N/A
64	**15 Termination rights and exit strategies**		
65	55. In case of cloud outsourcing of critical or important operational functions or activities, within the cloud outsourcing agreement the undertaking should have a clearly defined exit strategy clause ensuring that it is able to terminate the arrangement, where necessary. The termination should be made possible without detriment to the continuity and quality of its provision of services to policyholders. To achieve this, the undertaking should:	Undertakings 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 undertakings 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 undertakings 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
66	a. develop exit plans that are comprehensive, service based, documented and sufficiently tested (for example, by carrying out an analysis of the potential costs, impacts, resources and timing implications of the various potential exit options);	This is a customer consideration.	N/A
67	b. identify alternative solutions and develop appropriate and feasible transition plans to enable the undertaking to remove and transfer existing activities and data from the cloud service provider to alternative service providers or back to the undertaking. These solutions should be defined with regard to the	This is a customer consideration.	N/A

EIOPA Guidelines on Outsourcing to Cloud Service Providers

Google Workspace Mapping

	challenges that may arise because of the location of data, taking the necessary measures to ensure business continuity during the transition phase;		
68	c. ensure that the cloud service provider adequately supports the undertaking when transferring the outsourced data, systems or applications to another service provider or directly to the undertaking;	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 Google Account help page. In addition, **Data Export** is a feature that makes it easy to export and download a copy of your data securely from our Services.	Transition Term Data Export (Cloud Data Processing Addendum)
69	d. agree with the cloud service provider that once retransferred to the undertaking, its data will be completely and securely deleted by the cloud service provider in all regions.	On termination of the contractual relationship, Google will comply with the undertaking's instruction to delete Customer Data from Google's systems.	Deletion on Termination (Cloud Data Processing Addendum)