Chapter 2 - Privacy

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	Ref. ID	Questions related to reg. reference	Reg. reference	Offered / fulfilled by CSPs	Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.
Subchapter 2.1 CSP must provide Personal Data Protection in Accordance with European General Data Protection Regulations					
Data protection in public cloud environments is required to comply with the relevant European data protection regulations, in particular EU General Data Protection Regulation (EU) 2016/679 (GDPR), binding guidance of the European Data Protection Board, relevant European Court decisions, and European member state legislations. Within the EU and the European Economic Area (EU/EEA), GDPR is applicable for both, FIs (data-controller as cloud consumers) as well as for CSPs (data-processor). As data processors, CSPs are independent of their place of business, accountable to provide adequate technical and organisational security and compliance measures in the European market. Such measures should be state of the art, include data protection by design and default, and aim to even go beyond setting the benchmark. Furthermore, European citizens need to be able to trust that their FI take measures to respect and protect their privacy, including both contractual and technical aspects of such a relationship.	Ref 2.1.1	Do your customers unconditional access to documentation of your technical and organisational security and compliance measures for the European market?	GDPR: - Art. 28, 32 EBA/GL/2019/02 (Outsourcing): - Background Para. 44 - Chap. 3 Para. 16 - Chap. 4 Para. 38.b - Chap. 5 Accompanying documents, recital 8	YES	Google provides comprehensive external documentation and whitepapers detailing our security infrastructure and operational model. Refer to our Documentation page for technical documentation, including information on service configuration. (https://cloud.google.com/docs) Customers can review Google's Compliance Resource Center for more information and on-demand access to compliance and security resources. (https://cloud.google.com/security/compliance) Customers can also reference Appendix 2 in the Cloud Data Processing Addendum (CDPA), which describes various security measures that Google commits to implement and maintain. In addition to the security measures outlined in Appendix 2, the CDPA outlines customer's audit rights (sec. 7.5.2) to verify Google's compliance with its obligations under the CDPA. (https://cloud.google.com/terms/data-processing-addendum)
	Ref 2.1.2	Are these measures state of the art, including data protection by design and default?	GDPR: - Art. 25, 32 - Recital 78 ECJ Schrems 2: - Recital 108	YES	Refer to our whitepaper on safeguards for international data transfers with Google Cloud: https://services.google.com/fh/files/misc/safeguards_for_international_data_transfers_with_google_cloud.pdf Customers can also reference Appendix 2 in the Cloud Data Processing Addendum (CDPA), which describes various security measures that Google commits to implementing and maintaining. In addition to the security measures outlined in Appendix 2, the CDPA outlines customer's audit rights (sec. 7.5.2) to verify Google's compliance with its obligations under the CDPA. (https://cloud.google.com/terms/data-processing-addendum)
Subchapter 2.2 CSP should provide supplementary Measures to enable effective GDPR Compliance in 3rd Countries					
With regards to entering into contracts with CSPs established outside of the EU/EEA (3rd countries), the European Court of Justice (C-311/18 Schrems II) declared, that if applied standard contractual clauses ensure a GDPR equivalent environment for the individual, they can be an appropriate tool of transfer. Hence, the data controller (e.g. the FI) needs to ensure that the storage, transfer, and/or processing of data maintains GDPR equivalence and does not increase the risks of, for instance, unauthorised 3rd country processing. However, the outcome of adequacy evaluation and implementing contractual clauses potentially does not achieve a GDPR equivalent level of protection in the country where the CSP is established and/or where the data processing takes place. This is especially a challenge in countries where there are legislative requirements that authorizes public authorities to access data broadly beyond legitimate objective. Therefore, this may interfere with the contractually agreed confidentiality to access any personal data where the FI is the controller and is processed on its behalf by the CSP. The CSP should provide technical and organisational measures that ensure the compliance with GDPR in 3rd countries also.	Ref 2.2.1	Do technical and organisational measures of your organisation ensure an GDPR equivalent protection for personal data in 3rd countries? Please provide more details and references in the comment field.	GDPR: - Art. 44 subseq. ECJ Schrems 2: - Recital 134 EBA/GL/2019/02 (Outsourcing): - Background Para. 37 subseq. - Chap. 4 Para. 72, 83	YES	Refer to our whitepaper on safeguards for international data transfers with Google Cloud: https://services.google.com/fh/files/misc/safeguards_for_international_data_transfers_with_google_cloud.pdf Customers can also reference Appendix 2 in the Cloud Data Processing Addendum (CDPA), which describes various security measures that Google commits to implementing and maintaining. In addition to the security measures outlined in Appendix 2, the CDPA outlines customer's audit rights (sec. 7.5.2) to verify Google's compliance with its obligations under the CDPA. (https://cloud.google.com/terms/data-processing-addendum)
Subchapter 2.3 CSPs need to implement basic Security Principles					

In case a 3rd country can request access to personal data, according to the recommendations of the European Data Protection Board (EDPB) and the Standard Contractual Clauses 2021/914 of the European Commission (EU SCC 2021/914), data controllers and data processors should implement additional measures to ensure GDPR equivalent protection in the 3rd country. These technical measures are typically based on the principles of data security, data minimisation, anonymisation or pseudo-anonymisation. In the case of pseudonymisation, the CSP should support an approach where additional information for attribution of personal data to a specific data subject shall remain under the exclusive control of the FI. All CSPs and cloud operating models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) are in scope for these requirements.	Ref 2.3.1	In the case of pseudonymisation, does your organisation support an approach where additional information for attribution of personal data to a specific data subject remains under the exclusive control of the FI?	GDPR: - Art. 28, 44, 46, 32, 25 - Recital 26, 28, 29	YES	Cloud DLP supports three pseudonsmization techniques of de-identification, and generates tokens by applying one of three cryptographic transformation methods to original sensitive data values. Each original sensitive value is then replaced with its corresponding token. (https://cloud.google.com/dlp/docs/pseudonymization#supported-methods) For more information, see the Pseudonymisation page here: https://cloud.google.com/dlp/docs/pseudonymization
Subchapter 2.4 Cloud Services should facilitate Data Sovereignty by processing Data exclusively in the EU/EEA					
With the declared invalidation of the EU-US Privacy Shield by the European Court of Justice (Schrems II decision), FIs as cloud consumers should be able to apply data localisation to a certain country or geographic region, e.g. EEA. Furthermore, all cloud services should support storing and processing of customer and individual data exclusively in a dedicated country or geographic region e.g. in the EU/EEA.	Ref 2.4.1	Do your cloud services provide data localisation to a certain country or geographic region, e.g. EEA?	GDPR: - Art. 28, 44	YES	Google provides customers with choices about where to store their data. Once a location is chosen, Google will not store the customer data outside of the chosen region(s). Customers can also choose to use tools provided by Google to enforce data location requirements. Customers can reference Google's Data Location selection clause under the Service Specific Terms. (https://cloud.google.com/dlp/docs/pseudonymization) For more information, see our Data residency, operational transparency, and privacy for customers on Google Cloud Whitepaper. (https://services.google.com/fh/files/misc/googlecloud_european_commitments_whitepaper.pdf)
	Ref 2.4.2	Does your organisation provide tools to make data transfers visible, either initiated by the FI or the CSP, for whatever reason, and whether data travel within or outside of the EEA?	GDPR: - Art. 28 Para. 2	YES	Customers can find information about the location of Google's facilities and where individual GCP services can be deployed at our Global Locations page. (https://cloud.google.com/about/locations/) 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). See the Data Location selection clause under the Service Specific Terms. (https://cloud.google.com/terms/service-terms) Google recognizes that customers need visibilty into data transfers when using our services. Google facilitates that transparency, in part, by providing a host of privacy tools and functionalities, including: - Account management tools (e.g. My Account Dashboard, Activity Controls) - Operational tools (e.g. Cloud Console, Admin Console, Cloud Monitoring) - Access Transparency (https://cloud.google.com/access-transparency) - Access Approval (https://cloud.google.com/access-transparency) - Assured Workloads (https://cloud.google.com/assured-workloads) Customers 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 customers on Google Cloud Whitepaper.
	Ref 2.4.3	Does your organisation provide controls to the FI for validation in case personal data leaves or is accessed outside of the EEA, either knowingly or unknowingly?	GDPR: - Art. 28 Para. 2	YES	Refer to Ref 2.4.2
Subchapter 2.5 Global and regional Cloud Services must be made transparent to FIs					

CSP must make transparent what cloud services are operated only globally (so called Global services). In addition, CSP must make transparent if a cloud service necessarily requires transfers and/or processes personal data outside the EU. This information must be publicly accessible at any time, and it must not be limited to cloud services that potentially transfer customer data outside the EU as an essential function of the service. In addition, the CSP must proactively inform their FI customers if they add or alter any privacy and data protection features and/or capabilities as well as region expansion announcements as they are released.	Ref 2.5.1	Does your organisation provide full transparency over cloud services in your system that potentially or definitely transfers and/or processes personal data outside the EEA?	GDPR: - Art. 28 Para. 2, Art. 30 Para. 2	YES	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: https://cloud.google.com/about/locations/ Information about the location of Google's subprocessors' facilities is available on our Google Cloud subprocessors page: https://cloud.google.com/terms/subprocessors Google Cloud offers customers the ability to control where their data is stored. When the customers choose to configure resources in regions, for our key services, "Google will store that Customer Data at rest only in the selected Region" per our Service Specific Terms: https://cloud.google.com/terms/service-terms Using Assured Workloads, customers can create an environment and select their compliance regime. When customers create resources in the environment, Assured Workloads restricts the regions customers can select for those resources based on the compliance regime selected using Organization Policy. Assured Workloads configures the appropriate encryption services per workload depending on the compliance regime you chose. Aditionally, Assured Support; which is a value-added service to Premium or Enhanced Support ensures that only Google support personnel meeting specific geographical locations and personnel conditions support their workload when raising a support case or needing technical assistance.
	Ref 2.5.2	Is this information publicly accesible, even without a contract?	GDPR: - Art. 28 Para. 3.f	YES	See response to Ref 2.5.1
	Ref 2.5.3	Does your organisation proactively inform its customers if you add or alter any privacy / data protection compliance features and/or capabilities for the services, as well as any announcements about new region launches, as they become available to customers?	GDPR: - Art. 28 Para. 3.f	YES	Google Cloud announces new privacy / data protection compliance features and capabilities on the Google Cloud Compliance Blog and the Google Cloud Identity & Security Blog. Google continues to improve the security of 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, these updates apply to all customers at the same time. Google will not update our security measures in a way that results in a material reduction of the security of the services. Google Cloud announces new / future regions launches are announced on the Google Cloud Infrastructure Blog and listed on our Global Locations page
Subchapter 2.6 Provide robust and multi region-based Global Services					
CSP should ensure that global cloud services are hosted in multiple regions and must not rely on one region only. Alternatively, CSP must be transparent to their customers whether or not global services are localised in a single region.	Ref 2.6.1	Does your organisation provide cloud services declared a global services in multiple regions? Please describe in the comment field which of your global cloud services are hosted in one region only.	GDPR: - Art. 28, Art. 44	YES	Information about the location of Google's facilities and where individual Google Cloud services can be deployed, including in which region, is available at our Global Locations page (https://cloud.google.com/about/locations/).
Subchapter 2.7 Contractually agreed Data Processing Roles and Responsibilities must be adhered to by the CSPs					
Although CSPs aim to have differentiated approaches concerning the roles of being a data processor for the FI and a data controller for own interests (e.g. data analytics), ECUC asks CSPs to refrain from any data processing going beyond what has been contracted with respect to the data of the FI. When involving a CSP as 3rd party in the processing of customer data, the FI needs to be confident that the involvement of the additional processing party does not increase the risk of unauthorized processing/access to such data. CSPs also need to ensure that the processing of customer data remains within the limits of the contract with the FI. After contract expiration all data shall be returned and the CSP needs to certify that all data has been deleted.	Ref 2.7.1	Does your organisation offer full transparency on the role of the CSP referring to manage GDPR data (if CSP acts as a Data Processor), on the retention period of data processed, on the type of personal data processed, and if data profiling is done on data processed for each service in IaaS, PaaS or SaaS?	GDPR: - Art. 28 Para. 3, Art. 29 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 83	YES	Google Cloud is a processor of Customer Personal Data. Google Cloud's role as a processor, the data retention period, and the type of personal data processed are addressed in the Cloud Data Processing Addendum. Google commits to only access or use your data to provide the Services ordered by you and will not use it for any other Google products, services, or advertising. For more information on Google Cloud and our efforts in supporting our customers' compliance with GDPR, please see our GDPR resource center (https://cloud.google.com/privacy/gdpr).

	Ref 2.7.2	Does your organisation provide confirmation of customer data deletion following contract termination / expiry?	GDPR: - Art. 28 Para. 3 lit. G	PARTIAL	Google's process for data deletion upon termination /expiry is described in the "Data Deletion" section of our Cloud Data Processing Addendum (https://cloud.google.com/terms/data-processing-addendum). As specified in the CDPA, Google will comply with customers' instructions for deletion of customer data as soon as reasonably practicable and within a maximum period of 180 days, unless European law requires storage. Google's data deletion pipeline consists of four stages: 1) the Deletion Request, 2) Soft Deletion, 3) Logical Deletion from Active Systems, and 4) Expiration from Backup Systems. More specifically, logical deletion occurs in phases, beginning with marking the data for deletion in active storage systems immediately and isolating the data from ordinary processing at the application layer. Successive compaction and mark-and-sweep deletion cycles in Google's storage layers serve to overwrite the deleted data over time. Cryptographic erasure is also used to render the deleted data unrecoverable. Finally, backup systems containing snapshots of Google's active systems are retired on a standard cycle. For more information, see the Data Deletion on Google Cloud whitepaper (https://cloud.google.com/docs/security/deletion).
Subchapter 2.8 CSP should enable FIs to contract with EU based Legal Entities					
CSPs should offer FIs to contract with their legal entities based in the EU. Trilateral contractual relationships between FIs and both, the CSPs EU and non-EU based legal entities, contain uncertainties in terms of "Who is responsible for the control and contractual safeguarding of data transfers to countries outside the EU?" The ECUC regards the CSP EU based legal entities as the primary data processors for the personal data of the FI. If the CSP EU based legal entities send data to non-EU based CSP legal entities, the EU based legal entities are not only in breach of the contract but also act as data exporters, and thus being responsible to perform data transfer assessments and apply standard contractual clauses with their non-EU based entities.	Ref 2.8.1	Does your organisation offer FIs to contract with your legal entities based in the EU?	GDPR: - Art. 28 EBA/GL/2019/02 (Outsourcing): - Background Para. 41 - Chap. 4 Para. 67.a	YES	The Google Contracting Entity depends on the customer's billing address: https://cloud.google.com/terms/google-entity. Google Cloud EMEA Limited (an Irish company) is the service provider for customers based in most EU countries.
	Ref 2.8.2	Will your organisation apply Standard Contractual Clauses between your EU based and non-EU based entities?	GDPR: - Art. 28, 44, 46	YES	For information on Google's approach to EU Standard Contractual Clauses see here: https://services.google.com/fh/files/misc/gc_new_eu_scc.pdf
	Ref 2.8.3	When EU based legal entities of your organisation send data to your non-EU based legal entities, will you provide details of the data transfer assessments between these two parties?	GDPR: - Art. 46 EBA/GL/2019/02 (Outsourcing): - Background Para. 37, 41, 46 - Chap. 4 Para 68.d, 68.i	YES	For information on Google's approach to EU Standard Contractual Clauses see here: https://services.google.com/fh/files/misc/gc_new_eu_scc.pdf Refer to our Safeguards for International Data Transfers paper:https://services.google.com/fh/files/misc/safeguards_for_international_data_transfers_with_google_cloud.pdf More information about EU-US transfers is available upon request.
Subchapter 2.9 CSP must assess the Impact of 3rd Country Transfers					
The CSP must warrant that it has no reason to believe that the laws and practices in a 3rd country of destination, applicable to the processing of the personal data by one of its data importers, prevent such data importers from fulfilling its obligations under these clauses. This includes requirements to disclose personal data and/or measures authorising access by government authorities. It has to take due account of the specific circumstances of the transfer; the legislative requirements, practices, limitations and safeguards of countries of destination permitting data disclosure and/or access from authorities, practical experience with or knowledge of such requests and any contractual, technical or organisational supplementary safeguards put in place. The CSP shall conduct this assessment regularly (at least annually) in best efforts to continuously ensure compliance with obligations and to make the outcome with supporting information available to the FI upon request. A risk deemed low or medium by the CSP could be deemed differently by the FI due to its specific requirements. If the CSP has reason to believe that it can no longer comply with its commitments it shall immediately (at least within one day) inform the FI and identify appropriate protective measures. If instructed by the FI the data exporter should suspend the transfer in accordance with EU SCC 2021/914 Recital 17. This CSP transfer impact assessment must be performed independently of any assessment of the FI in accordance with accountability obligations in its provider selection process.	Ref 2.9.1	Does your organisation assess specific circumstances of the transfer regularly and ad hoc (the legislative requirements, practices, limitations and safeguards of countries of destination permitting data disclosure and/or access from authorities)?	GDPR: - Art. 28, 44, 46, 48 ECJ Schrems 2 EBA/GL/2019/02 (Outsourcing): - Background Para 37, 41, 46 - Chap. 4 Para 68.d, 68.i	YES	Refer to the Google Cloud EU Standard Contractual Clauses: https://cloud.google.com/terms/sccs/eu-p2p-google-exporter. Google Cloud will comply with its obligations in the EU Standard Contractual Clauses (e.g. Clause 14(a)-(c)). For information on Google's approach to European Standard Contractual Clauses see here: https://services.google.com/fh/files/misc/gc_new_eu_scc.pdf More information about EU-US transfers is available upon request.
	Ref 2.9.2	Does your organisation provide the outcome of your assessment with supporting information to the FI upon request?	GDPR: - Art. 28	PARTIAL	Although we are unable to provide customers with our own internal assessments, we are able support customers with specific questions. We firmly believe that Google Cloud's Standard Contractual Clauses, along with our other safeguards and commitments, provide our customers' data with adequate protection when it is transferred internationally.
	Ref 2.9.3	If your organisation can no longer comply with your commitments, will you immediately (at least within one day) inform the FI and identify appropriate protective measures?	GDPR: - Art. 28	PARTIAL	Google Cloud will comply with its obligations in the EU Standard Contractual Clauses (e.g. Clause 8.1(c) and Clause 14(e)). Specifically, Google will immediately inform the data exporter if it is unable to follow the data exporter's instructions.
	Ref 2.9.4	If instructed by the FI, will your organisation suspend the transfer in accordance with EU SCC 2021/914 Recital 17?	GDPR: - Art. 28, 44, 46	YES	Google Cloud will comply with its obligations in the EU Standard Contractual Clauses (Clause 14(f)).

Subchapter 2.10 CSP should achieve holistic Effectiveness of Encryption

In its Guideline on supplementary measures the EDPB emphasises the use of effective encryption as an adequate supplementary measure to the Standard Contractual Clauses to ensure adequate and effective protection in case of a data transfer outside of the EU/EEA or 3rd countries with established equivalence. Therefore, the ECUC encourages CSPs to seek and proceed in developing new encryption techniques and other data protection measures to protect the data adequately and effectively at any given time.	Ref 2.10.1	Does your organisation plan or is in progress of developing new encryption techniques and other data protection measures to adequately and effectively protect the data at any given time?	GDPR: - Art. 28, 32 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para 68.e	YES	Google continues to improve the security of our services to enable our customers to take advantage of the most up-to-date technology, including new advancements in encryption. Google Cloud announces new privacy / data protection compliance features and capabilities on the Google Cloud Compliance Blog and the Google Cloud Identity & Security Blog.
Hence, guaranteeing encryption and ensuring that the encryption keys are kept under the full control of an EU entity is an option to legally transfer personal data e.g. data transferred to the US. However, such a proposed approach may only address risks associated with data that is in transit and/or data at rest. Therefore, the EDPB questions the effectiveness of encryption regarding preventing access to data being processed (e.g. data in use). Bring-your-own-key and hold-your-own-key approaches (using HSM technologies) are valuable first steps, but the CSP need to find a holistic approach towards trusted computing giving the FI the opportunity to stay fully in control and deny technically any 3rd party and even the CSP potential access to personal data in clear text.	Ref 2.10.2	Will your organisation guarantee that encryption of data in transit and data at rest as well as corresponding encryption keys can be kept under the full control of an EU entity?	GDPR: - Art. 28, 32	PARTIAL	Google Cloud applies encryption at rest and in transit by default. To gain more control over how data is encrypted, Google Cloud customers can use Cloud Key Management Service to generate, use, rotate, and destroy encryption keys according to their own policies. With Cloud EKM (https://cloud.google.com/kms/docs/ekm), customers can use keys that they manage within a supported external key management partner to protect data within Google Cloud. Customers control the location and distribution of their externally managed keys. Externally managed keys are never cached or stored within Google Cloud. Instead, Cloud EKM communicates directly with the external key management partner for each request. Refer to the documentation above for information about which Google Cloud services support Cloud EKM. Google provides customers with tools that facilitate ubiquitous data encryption which delivers unified control over data at-rest, in-use, and in-transit, all with keys that are under your control.
	Ref 2.10.3	Will your organisation guarantee that encryption services for data in use and corresponding encryption keys can be kept under the full control of an EU entity?	GDPR: - Art. 28, 32	PARTIAL	See reponse to Ref 2.10.2
	Ref 2.10.4	Will your organisation guarantee that FIs can choose to deny your support personnel and / or any 3rd party access customer data in clear text?	GDPR: - Art. 32, 32	PARTIAL	Key Access Justification works with External Key Manager. It provides a detailed justification each time one of your keys is requested to decrypt data, along with a mechanism for you to explicitly approve or deny providing the key using an automated policy that you set. Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency. Refer to the documentation above for information about which Google Cloud services offer Key Access Justification and Access Approval.

Subchapter 2.11 Disclosure Request must be challenged by the CSP

The CSP shall review the legality of disclosure requests and challenge them if it concludes that the request is unlawful. The CSP therefore needs to pursue possibilities of appeal, seek interim measures with an objective to suspend the request and not disclose the personal data requested but instead forward the request to the individual FI. If disclosing, the CSP shall provide the minimum amount permissible. The CSP shall notify the FI and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it receives a legally binding request or becomes aware of any direct access by public authorities. Prior information should be given as soon as the CSP is made aware to give the FI the opportunity to object or limit access (CSP should support embedding a kill switch or similar technologies or procedures to block autonomously 3rd country access as soon such is identified). Furthermore, the CSP should deny access before the affected FI was able to take actions. If the CSP is prohibited from notifying the FI and/or the data subject under the laws of the country of destination, the CSP shall ensure best efforts to obtain a waiver of the prohibition or forward the request to the FI, with the ambition to communicate as much information as possible and as soon as possible.	Ref 2.11.1	Does your organisation review the legality of disclosure requests and challenge them if you hold the request being unlawful?	GDPR: - Art. 29, 47	YES	Information about Google's practices around government requests for data is available in our Government Requests for Cloud Customer Data whitepaper. (https://services.google.com/fh/files/misc/google_cloud_governmentrequestsfor_cloud_customer_data_v2_1018.pdf)
	Ref 2.11.2	If in doubt, will your organisation suspend the request and not disclose the personal data requested but instead forward the request to the individual FI?	GDPR: - Art. 29, 47	YES	If Google receives a government request, Google will: - attempt to redirect the request to the customer - notify the customer prior to disclosure unless prohibited by law - comply with the customer requests to oppose disclosure - only disclose if strictly necessary to comply with legal process More information about Google's practices around government requests for data is available in our Government Requests for Cloud Customer Data whitepaper. (https://services.google.com/fh/files/misc/google_cloud_governmentrequestsfor_cloud_customer_data_v2_1018.pdf)
	Ref 2.11.3	If there is no choice other than to fulfil the disclosure request, will your organisation endeavour to disclose the minimum amount of data possible?	GDPR: - Art. 29, 47, 25, 28	YES	See response to Ref 2.11.2

	Ref 2.11.4	Will your organisation notify the FI and, where possible, the data subject promptly if you receive a legally binding request or become aware of any direct access by public authorities?	GDPR: - Art. 28, 12	YES	See response to Ref 2.11.2
	Ref 2.11.5	Will your organisation enable the FI to object or limit access to this data prior to disclosure?	GDPR: - Art. 28	YES	See response to Ref 2.11.2
	Ref 2.11.6	Will your organisation deny access to the requestor before the affected FI is able to take action?	GDPR: - Art. 28 - Art. 44 subseq.	PARTIAL	Google will, to the extent allowed by law and by the terms of the request, comply with a customer's reasonable requests regarding its efforts to oppose a request, such as the customer filing an objection to the disclosure with the relevant court and providing a copy of the objection to Google. If Google notifies the customer of a legal request and the customer subsequently files an objection to disclosure with the court and provides a copy of the objection to Google, Google will not provide the data in response to the request if the objection is resolved in favor of the customer. Note that certain jurisdictions may have different procedures and are handled on a case-by-case basis.
	Ref 2.11.7	Does your organisation provide a kill switch or similar technology or procedure so the FI can block autonomously 3rd country access as soon such is identified?	GDPR: - Art. 28 - Art. 44 subseq.	YES	See response to Ref 2.10.4 Information about Google Cloud's data sovereignty capabilities and solutions is available at https://cloud.google.com/blog/products/identity-security/how-google-cloud-is-addressing-data-sovereignty-in-europe-2020 and https://cloud.google.com/blog/products/identity-security/advancing-digital-sovereignty-on-europes-terms
	Ref 2.11.8	If your organisation is prohibited from notifying the FI and/or the data subject under the laws of the country of destination, will your organisation ensure best efforts to obtain a waiver of the prohibition or forward the request to the FI, with the ambition to communicate as much information as possible and as soon as possible to the FI?	GDPR: - Art. 28 - Art. 44, 48	YES	See response to Ref 2.11.2
Subchapter 2.12 Transparency Reports must be provided by the CSPs					
Where legally permissible in destination country, the CSP agrees to provide the FI, in regular intervals for the duration of the contract, with as much relevant information as possible on the requests received, in particular, number of requests, type of data requested, requesting authorities, whether requests have been challenged and the outcome of such challenges, etc. If the CSP acts as a data processor, it shall forward the information to the FI as data controller as quickly as possible.	Ref 2.12.1	Will your organisation fully provide the information outlined in Chapter 2.12?	GDPR: - Art. 46(1), (2c) ECJ Schrems 2: - Recital 109, 139, 143 EDPB Sup. Mea.: - marginal no. 133 subseq.	YES	Google was the first cloud provider to publish regular transparency reports on government requests for customer information, as well as requests for Google to remove content from publication. In our Transparency Reports, we share our data about how the policies and actions of governments and corporations affect privacy, security, and access to information. (https://transparencyreport.google.com/user-data/overview)
Subchapter 2.13 CSP should provide Warrant Canary on Request of FI					
Upon request, the CSP should provide information through a *Warrant Canary* or similar process to inform each FI on a regular basis (e.g. at least every 24 hours) that no access requests have been received from authorities acting against GDPR. This may be done e.g. by sending a cryptographically signed message informing the FI that as of a certain date and time it has received no order to disclose personal data or the like, if this is permitted by the regulation of the CSP place of business in a 3rd country. The CSP must ensure that its private key for signing the Warrant Canary is kept safe and that it cannot be forced to issue false Warrant Canaries by the regulations of the 3rd country, e.g. by appointing a person outside of the 3rd country jurisdiction. The absence of an update of this notification will indicate from FI perspective that the CSP may have received an order and enable the FI to take defence actions.	Ref 2.13.1	Does your organisation provide a Warrant Canary or similar process to inform each FI regularly (e.g. at least every 24 hours) that no access requests have been received from authorities acting against GDPR? Please specify the process and the frequency your organisation is offering in the comment field.	GDPR: - Art. 46(1), (2c) ECJ Schrems 2: - Recital 139 third sentence EDPB Sup. Mea.: - marginal no. 116.	NO	We will notify the customer before their customer data is disclosed unless such notification is prohibited by law, could obstruct a government investigation, or lead to death or serious physical harm to an individual. Where prior notification by Google is prohibited under applicable law, it is Google's policy to notify the customer when any prohibition is eventually lifted, such as when a statutory or court ordered disclosure prohibition period has expired. This notification typically goes to the Google Cloud customer's point of contact. More information about Google's practices around government requests for data is available in our Government Requests for Cloud Customer Data whitepaper. https://services.google.com/fh/files/misc/google_cloud_governmentrequestsfor_cloud_customer_data_v2_1018.pdf
	Ref 2.13.2	If your organisation provides a Warrant Canary process, will your organisation ensure that the private key for signing the Warrant Canary is kept safe and that it cannot be forced to issue false Warrant Canaries by the regulations of the 3rd country?	GDPR: - Art. 46(1), (2c) ECJ Schrems 2: - Recital 139 third sentence EDPB Sup. Mea.: - marginal no. 116.	NO	Google provides a number of technical tools that give customers greater control of their own data in relation to government requests. These include enhanced customer controls (Cloud EKM, Key Access Justifications, Client-Side Encryption), cryptographic key management (Cloud KMS, Cloud HSM), and access controls (BeyondCorp Enterprise, Access Transparency, Access Approval). More information about Google's practices around government requests for data is available in our Government Requests for Cloud Customer Data whitepaper. https://services.google.com/fh/files/misc/google_cloud_governmentrequestsfor_cloud_customer_data_v2_1018.pdf

Subchapter 2.14 Personal Data Protection Audits should be supported

The CSP shall be able to demonstrate compliance with its contractual safeguard provisions. In particular, the CSP shall keep appropriate documentation on the processing activities carried out on behalf of the FI. The CSP shall make available all information necessary for the FI to demonstrate compliance with the obligations set out in these Clauses and at the FIs request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may consider relevant certifications held by the data importer. The FI may choose to conduct the audit by itself, mandate an independent auditor or choose to perform the audit in a pooled audit together with other FIs. Audits may include inspections at the premises or physical facilities of the CSP and shall, where appropriate, be carried out with reasonable notice.	Ref 2.14.1	Will your organisation make available all information necessary for the FI to demonstrate compliance with the contractual obligations by the means of an audit of the processing activities at reasonable intervals?	GDPR: - Art. 5, 28 (3h), 30, 46(1), (2c) EBA/GL/2019/02 (Outsourcing): - Recital Para. 85 ff.	YES	Google also grants customers audit rights in the Cloud Data Processing Addendum. (https://cloud.google.com/terms/data-processing-addendum)

Subchapter 2.15 Personal Data Breaches must be reported immediately

In the event of a personal data breach processed for an FI including government request, the CSP shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The CSP shall also notify the FI without undue delay after having become aware of the breach and allow the FI to report the breach at the latest within 72h to the respective regulator. Such notification shall contain a description of the nature of the breach including categories and numbers of affected data subjects and personal data, the details of a data protection officer or contact point where more information can be obtained, the likely consequences of the affected breach and the measures taken or proposed to address the breach and mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, CSP shall send an initial notification containing the information then available and deliver further information as it becomes available without undue delay. The first notification of the breach must not be delayed by the CSP performing internal investigations on the question if this is a breach that needs to be notified as the assessment of this question is a prerogative of the FI as data controller.	Ref 2.15.1	In the event of a personal data breach, will your organisation notify the FI without undue delay after having become aware of the breach?	GDPR: - Art. 33 (2) EDPB WP 250 GL on pers. data breach: - p. 13	YES	Google notifies customers 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. (https://services.google.com/fh/files/misc/data_incident_response_2018.pdf)
	Ref 2.15.2	Will your organisation allow the FI to report the breach latest within 72h to the respective regulator?	GDPR: - Art. 33 Para. 2 - Recital 85 Para. 2, 87 EDPB WP 250 GL on pers. data breach: - p. 13	YES	See Ref 2.15.1
	Ref 2.15.3	Will such notification contain a description of the nature of the breach including categories and numbers of affected data subjects and personal data, as well as the likely consequences of the affected breach and the measures taken or proposed to address the breach and mitigate its possible adverse effects?	GDPR: - Art. 33 Para. 3 EDPB WP 250 GL on pers. data breach: - p. 13 subseq.	YES	See Ref 2.15.1. See also secion 7.2 of the Cloud Data Processing Addendum. (https://cloud.google.com/terms/data-processing-addendum)
	Ref 2.15.4	If it is not possible to provide all information at the same time, will your organisation send an initial notification containing the information then available and deliver further information as it becomes available without undue delay?	GDPR: - Art. 33 Para. 4 EDPB WP 250 GL on pers. data breach: - p.15	YES	See Ref 2.15.1

Subchapter 2.16 CSP Personnel accessing Customer Data must be traceable

In the event where CSP support personnel need access to cloud services, FIs must be able to grant access, monitor and trail access made by such personnel. The CSP must provide details to trace and protocol these support access activities. There must be no backdoor where CSP support personnel accesses customer data/cloud services without the ability to trail. Amongst others these activities include internal support networks. The CSP must provide a reliable "technical vault mechanism" including surrounding controls and processes around to prevent unauthorized (administrative) access to customer data as well as meta data by any support party, CSP support personnel and sub-contractors.	Ref 2.16.1	In the event where your organisation´s support personnel and / or sub-contractors need access to customer data in the cloud services, do you enable FIs to grant access, monitor and trail such access to customer data?	GDPR: - Art. 32 Para. 4 ECJ Schrems 2: - Recital 134	YES	The "Managing Google's Access to your Data" section of our Trusting your data with Google Cloud whitepaper explains Google's data access processes and policies. In addition, you can also monitor and control the limited actions performed by Google personnel on your data using these tools: 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). Access Approval is a feature that enables you to require your explicit approval before Google support and engineering teams are permitted access to your customer content. Access Approval provides an additional layer of control on top of the transparency provided by Access Transparency. Information about Google Cloud's data sovereignty capabilities and solutions is available at https://cloud.google.com/blog/products/identity-security/how-google-cloud-is-addressing-data-sovereignty-in-europe-2020 and https://cloud.google.com/blog/products/identity-security/advancing-digital-sovereignty-on-europes-terms
	Ref 2.16.2	Does your organisation provide means to trace and protocol such support accesses by your support personnel and / or sub-contractors?	GDPR: - Art. 32 Para. 4 ECJ Schrems 2: - Recital 134	YES	See Ref 2.16.1
	Ref 2.16.3	Will the ability to track and trace support personnel and / or subcontractor activities be applicable to your organisation´s internal management and support networks?	GDPR: - Art. 32 Para. 4 ECJ Schrems 2 Rn. 134	YES	See Ref 2.16.1
	Ref 2.16.4	Does your organisation provide a reliable "technical vault mechanism" including surrounding controls and processes around to prevent unauthorized (administrative) access to customer data as well as meta data by any support party, CSP support personnel and sub-contractors?	GDPR: - Art. 32 Para. 2, 3 ECJ Schrems 2: - Recital 134	YES	See Ref 2.16.1. In addition, Cloud Audit Logs are encrypted at rest by default and reside in highly protected storage, resulting in a secure, immutable, and highly durable audit trail. The service is also coupled with Google Cloud's Access Transparency service, which surfaces near real-time logs of GCP administrator access to your systems and data.

Chapter 3 - Security

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	Ref. ID	Questions related to reg. reference / recognised standard (examples)	Reg. reference / recog. stand. (examples)	Offered / fulfilled by CSPs	Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.
Subchapter 3.1 Strong and Transparent Data at Rest Security					
Data at Rest refers to the storing of data. To fulfil this basic need for cloud customers, transparent and strong security in the cloud is a necessity. Therefore, CSPs should provide solutions to ensure adequate security is in place.	Ref 3.1.1	Is data at rest security enabled by default, when setting up an account?	CSA CCM v4.0.5: - CEK-04	YES	Google encrypts Google Cloud customer data stored at rest by default, with no additional action required from customers. More information is available on the Google Cloud Encryption at rest page. (https://cloud.google.com/docs/security/encryption/default-encryption)
	Ref 3.1.2	If data at rest security is enabled, can your organisation provide the details of the implemented data security measures?	CSA CCM v4.0.5: - CEK-04 ff	YES	Google has policies and documentation in place that outline our cryptography and encryption protocols, including details on security measures. More information is available on the Google Cloud Encryption at rest page. (https://cloud.google.com/docs/security/encryption/default-encryption)
	Ref 3.1.3	Does your organisation keep your data at rest security up to date with new regulations?	CSA CCM EBA/GL/2019/04 (ICT)	YES	Google's security engineering organization ensures effectiveness of the information protection program through program oversight. As part of the program oversight, the organization establishes and communicates Objective Key Results (OKRs) and updates of Google's security plan, which may include updates to our services based on identified, applicable legal standards and regulations.
	Ref 3.1.4	Does your organisation notify the customers if new security regulations are adopted? Please specify how in the comment field.	CSA CCM EBA/GL/2019/04 (ICT)	YES	Compliance with new security regulations are shared with customers on our Compliance Resource Center, which is publicly available at https://cloud.google.com/security/compliance.
Firstly, a data encryption methodology should be implemented in such a way that the CSP cannot be forced to disclose the keys to decrypt customer data without approval, consent or knowledge of the data owners. More precisely, a CSP should employ at least a level three, 140-2 Financial Information Processing Standard (FIPS) Hardware Security Module (HSM) which supports state of the art cryptographic processes as well as provides a scalable and managed Key Management Service (KMS) based on HSMs, including key import and re-import, rotation, re-encryption, grouping, and labelling. A CSP should also offer multiple methods for customers to encrypt data at rest, for example: - Supply Your Own Key upon each request - Bring Your Own Key into CSPs HSM - External Key Management where key encryption keys reside outside CSPs HSM - Privately hosted HSMs in a co-location.	Ref 3.1.5	Does your KMS provide the customer with exclusive control? Please specify your approach in comment field.	CSA CCM v4.0.5: - CEK-04	YES	Customers may use Cloud EKM to maintain exclusive control over their encrypted data. With Cloud EKM, the customer manages access to externally-managed keys. To use an externally-managed key to encrypt or decrypt data in Google Cloud, customers must grant the Google Cloud project explicit access to use the key manager.
	Ref 3.1.6	Does your organisation support FIPS 140-2 Level 3 HSM technology in your systems? Please specify if it is internal, external or both in the comment field.	CSA CCM v4.0.5: - CEK-06, 08, 10	YES	Customers can generate hardware keys in a cluster of FIPS 140-2 Level 3 Hardware Security Modules (HSMs). Customers have control over the rotation period, IAM roles and permissions, and organization policies that govern their keys. When customers create HSM keys using Cloud HSM, Google manages the HSM clusters so customers don't have to. Customers can use their HSM keys with over 30 compatible Google Cloud resources —the same services that support software keys. For the highest level of security compliance, customers should use hardware keys. (https://cloud.google.com/kms/docs/compatible-services)
	Ref 3.1.7	If your organisation supports an external HSM, does this limit your service offering? Please specify the not supported services in the comment field.	CSA CCM v4.0.5: - CEK-06, 08, 10	YES	Google Key Management services support all methods for customers to encrypt data at rest: from Cloud KMS, to Cloud HSM, External KMS based on 3rd party HSM partners, or Hosted HSM option with our product HPH. When customers decide to use External Key Manager with 3rd party HSM providers, it limits the set of Google Cloud services customers would be able to utilize and also would require them to plan their deployment accordingly with the right SLO paying attention to the throughput, performance and latency, and supportability of 3rd party HSM vendors in mind.
	Ref 3.1.8	Does your organisation's KMS provide to the customer scalability?	CSA CCM v4.0.5: - CEK-06, 08, 10	YES	Cloud KMS, together with Cloud HSM and Cloud EKM, supports a wide range of compliance mandates that call for specific key management procedures and technologies. It does so in a scalable, cloud-native way, without undermining the agility of the cloud implementation.
	Ref 3.1.9	Does your organisation's KMS provide to the customer key operations?	CSA CCM v4.0.5: - CEK-06, 08, 10	YES	Customers can encrypt data in BigQuery and Compute Engine with encryption keys that are stored and managed in a third-party key management system that's deployed outside Google's infrastructure. External Key Manager allows customers to maintain separation between their data at rest and their encryption keys while still leveraging the power of cloud for compute and analytics.
	Ref 3.1.10	Does your organisation's KMS provide to the customer encryption?	CSA CCM v4.0.5: - CEK-06, 08, 10	YES	Customers have the ability to manage keys the same way they would on premise, and allows for external keys in addition to full customization of encryption type.

	Ref 3.1.11	Does your organisation´s KMS provide to the customer signatures?	CSA CCM v4.0.5: - CEK-06, 08, 10	YES	Cloud KMS provides the following functionality related to creating and validating digital signatures. - Ability to create an asymmetric key with key purpose of ASYMMETRIC_SIGN. Cloud KMS keys for asymmetric signing support both elliptic curve signing algorithms and RSA signing algorithms. - Ability to create a digital signature. - Ability to retrieve the public key for an asymmetric key. Cloud KMS does not directly provide the ability to validate a digital signature. Instead, you validate a digital signature using openly available SDKs and tools, such as OpenSSL. These SDKs and tools require the public key that you retrieve from Cloud KMS. For information on how to use open SDKs and tools, see validating an elliptic curve signature and validating an RSA signature. (https://cloud.google.com/kms/docs/digital-signatures)
	Ref 3.1.12	Does your organisation´s KMS provide to the customer meta data?	CSA CCM v4.0.5: - CEK-06, 08, 10	PARTIAL	Per the link below, Cloud KMS helps guard against data corruption and to verify that data can be decrypted successfully. Cloud KMS periodically scans and backs up all key material and metadata. Key metadata: Resource names, properties of KMS resources such as IAM policies, key type, key size, key state, and any data derived from the above. Key metadata can be managed differently than the key material. (https://cloud.google.com/docs/security/key-management-deep-dive)
Secondly, it should be transparent to cloud customers which encryption keys are used for specific actions or on what grounds they are updated, when data assets are encrypted and by whom, thus ensuring auditability. A CSP should offer customers organisation-wide encryption policies and a central place to define Data at Rest encryption for all services. Furthermore, it should enable all services to support the cryptographic key management options mentioned above as well as provide access sovereignty and access transparency logs to justify usage of cryptographic keys and provide a holistic dashboard for all key involvement.	Ref 3.1.13	Does your organisation´s Key Management Service support different cryptographic methods? Please list them in the comment field.	CSA CCM v4.0.5: - CEK-12	YES	Google's Cloud key Management lets customers manage symmetric and asymmetric cryptographic keys for their cloud services the same way they do on-premises. Customers can generate, use, rotate, and destroy AES256, RSA 2048, RSA 3072, RSA 4096, EC P256, and EC P384 cryptographic keys.
	Ref 3.1.14	Does your organisation ensure the immutability of each cryptographic key operation? Please provide the details in the commentary field.	CSA CCM v4.0.5: - CEK-12	YES	Cloud KMS takes extra steps to protect encryption keys at rest by encrypting each encryption key using another cryptographic key called a key encryption key (KEK). To learn more about this technique, refer to envelope encryption. (https://cloud.google.com/kms/docs/envelope-encryption) Each Cloud KMS cryptographic operation includes automatic checks for data corruption. If corruption is detected, the operation is aborted and a detailed error is logged. These automatic protections are important, but they don't prevent client-side data corruption. For example, data corruption during encryption can lead to data that can't be decrypted. (https://cloud.google.com/kms/docs/data-integrity-guidelines)
	Ref 3.1.15	Does your organisation provide data at rest encryption as an enforced system policy for all services?	CSA CCM v4.0.5: - CEK-04	YES	See response to Ref 3.1.1
	Ref 3.1.16	Can your organisation provide access control and transparency of all keys access operations? Please provide in the comment field the services which are being supported by the above mentioned data at rest encryption.	CSA CCM v4.0.5: - CEK-08, 10, 12	YES	Google believes that customers should have a robust level of control over data stored in the cloud and we've developed product capabilities that enhance customer control over their data and provide expanded visibility into when and how their data is accessed. To that end, Google Cloud has implemented access controls designed to ensure that each of the data access pathways functions as intended. More information can be found in our Trusting your data with Google Cloud whitepaper. (https://services.google.com/fh/files/misc/072022_google_cloud_trust_whitepaper.pdf)
	Ref 3.1.17	In the case of a systemic failure of the KMS rendering our data become inaccessible, does your organisation provide support? Please provide in the comment field in which way you can provide support.	CSA CCM v4.0.5: - CEK-13	YES	Customer support for all platforms is provided in the event of an outage. (https://cloud.google.com/support)
	Ref 3.1.18	Does your organisation provide central monitoring / reporting on key management?	CSA CCM v4.0.5: - CEK-01	YES	Cloud Monitoring can be used to monitor operations performed on resources in Cloud Key Management Service. For more information, see our Using Cloud Monitoring with Cloud KMS page. (https://cloud.google.com/kms/docs/monitoring)
	Ref 3.1.19	Does your organisation offer a single pane of glass view on the state of encryption of all encrypted data?	CSA CCM v4.0.5: - CEK-12	YES	Every single option (except Hosted HSM) is available via a single pane of glass. In addition, Google offers key tracking services to understand the relationship with key assets and resources to help them manage their encrypted data and keys more efficiently.

Subchapter 3.2 Strong and Transparent Data in Transit Security

For FIs currently using public cloud services, it is often unclear to them where their data is transferred and how it is secured in transit. However, it should always be transparent to the FI how and where their data is being transferred, particularly the security measures in place to protect data-in-transit. The CSP should use state of the art security to secure data-in-transit, e.g., TLS version 1.3. Hence, vulnerable data security protection should be avoided.	Ref 3.2.1	Does your organisation implement technical measures to protect data-in-transit between on premise and your cloud infrastructure, within your cloud infrastructure, and towards third parties (e.g., Internet)? Please elaborate the technical measures for each data-in-transit type in the comment field.	CSA CCM v4.0.5: - CEK-03 - DSP-10 - UEM-12	YES	Google encrypts data-in-transit at several levels. All data is encrypted while it is "in transit", traveling over the Internet and across the Google network between data centers. See the Google Cloud Encryption in Transit page for more information. (https://cloud.google.com/docs/security/encryption-in-transit)
	Ref 3.2.2	Does your organisation use state-of-the-art cryptographic methods to ensure data-in-transit security? Please elaborate the details of the implemented cryptographic method ensuring data-in-transit security in the comment field.	CSA CCM v4.0.5: - CEK-03 - DSP-10 - UEM-12	YES	See response to Ref 3.2.1
To provide clarity on the data transport architecture, the CSP should provide a consistent, central place to configure and monitor data-in-transit security, rather than only per individual service.	Ref 3.2.3	Does your organisation provide a centralized management console to configure and monitor data-in-transit security e.g. native integration of market CASB? Please provide more information in the comment field.	CSA CCM v4.0.5: - CEK-03 - DSP-10 - UEM-12	YES	Google offers customers control and monitoring functionality via the Cloud Console, where they can configure protections for their data when it is in transit between Google Cloud and their data centers, or in transit between their applications that are hosted on Google Cloud and user devices.
Also, a precise description of the CSP's internal data transfer channels and applied security measures should be made transparent to the FI.	Ref 3.2.4	Can your organisation specify for your internal data transfer the details of transfer channels and applied security measures? If yes, please give specification (reference) in CSP comment field.	CSA CCM v4.0.5: - CEK-03 - DSP-10 - UEM-12	YES	Google's data centers are connected via high-speed private links to provide secure and fast data transfer between data centers. Transmissions consist of service calls between front-end and back-end machines that use secure authentication over a proprietary SSL-based protocol that supports AES-128.
In addition, for each cryptographic process, a clear justification should be available and included in log files, e.g., certificate renewal.	Ref 3.2.5	Can your organisation provide evidence for implemented cryptographic processes around certificates, e.g., logfiles of certificate operations?	CSA CCM v4.0.5: - CEK-03 - DSP-10 - UEM-12	YES	All certificates issued by a cloud CA (Certificate Authority Service) are logged via cloud audit log. All certificates managed by Google (cloud Certificate Manager) are also logged.
Subchapter 3.3 Fully Featured Logging and Monitoring					
To ensure full control of customer data assets, robust, and complete audit logging of all cloud application and service activity is required. This applies to both customer and CSP actions and the retention time should be defined by the customer. Logging and Monitoring includes customer service access (Access Transparency with approvals), CSP and customer admin access (Admin Activity/Read/Write), as well as data that have been accessed (Data Access/Read/Write).	Ref 3.3.1	Does your organisation provide complete audit logging of all cloud application and service activity?	CSA CCM v4.0.5: - LOG-10, 11	YES	Cloud Audit Logs provides the following audit logs for each Cloud project, folder, and organization: - Admin Activity audit logs - Data Access audit logs - System Event audit logs - Policy Denied audit logs https://cloud.google.com/logging/docs/audit
	Ref 3.3.2	Does your organisation provide the logging of both customer and CSP actions?	CSA CCM v4.0.5: - LOG-01 ff	YES	Google Cloud services write audit logs that record administrative activities and accesses within customer's Google Cloud resources. More information visit: https://cloud.google.com/logging/docs/audit
	Ref 3.3.3	Does your organisation ensure integrity of logging?	CSA CCM v4.0.5: - LOG-01 ff	YES	Google restricts physical and logical access to audit logs to authorized users only through the use of access control lists within the logging system. Audit information is protected from unauthorized modification and deletion through the use of checksums. Google maintains an automated log collection and analysis tool to review and analyse log events. Google also maintains policies on log retention and log security requirements.
If only the CSP accesses customer assets, the customer should be provided with functionality to effectively control the access for this specific resource before any access happens.	Ref 3.3.4	Does your organisation provide a control mechanism which requires the approval from the customer prior to any admin access being granted?	CSA CCM v4.0.5: - LOG-01 ff	YES	Google has policies and procedures in place for security logging requirements, rules on log data usage, and monitoring alerts. Google also discusses monitoring in our security whitepaper: https://cloud.google.com/security/overview/whitepaper In addition, customers can leverage both Access Transparency and Access Approval for controlling access permissions. Specifically, Access Approval is a feature that enables customers to require their explicit approval before Google support and engineering teams are permitted access to their customer content. https://cloud.google.com/access-transparency

A CSP should, for all services, consistently log identity, performed action, service usage, corresponding purpose, and involved data. Cloud customers should be able to access comprehensive logs to the service related activities on the platform; this could be provided via for instance an Application Programming Interface (API), a Graphical User Interface (GUI) or some other mechanisms to integrate with their own security logging systems.	Ref 3.3.5	Does your organisation provide a centralised Security Monitoring service where all logs and alerts are generated either by user activities, service activities, data activities data, etc. and can be actively monitored and tracked?	CSA CCM v4.0.5: - LOG-03	YES	Google maintains a security monitoring program to detect and report security related events in our infrastructure and applications. Google Cloud customers can leverage a number of tools including: - The Security Command Center, which allows them to gain insight into the security state of their Google Cloud assets. (https://cloud.google.com/security-command-center/docs/) - Cloud Audit Logs, which provides the same level of transparency over administrative activities and accesses to data in Google Cloud as in on-premises environments. Every administrative activity is recorded on a hardened, always-on audit trail, which cannot be disabled by any rogue actor. (https://cloud.google.com/audit-logs/) - Cloud Monitoring, which supports monitoring of hybrid and multicloud environments. (https://cloud.google.com/monitoring)
Furthermore, customer log data should not be shared with 3rd parties without the consent of the customer.	Ref 3.3.6	Does your organisation share logging data with any 3rd parties or subcontractors without upfront consent of the customers? Please elaborate in comment field which cases and why you need to share logging data with which 3rd parties.	CSA CCM v4.0.5: - LOG-04	PARTIAL	If logging data is Customer Data under the Cloud Data Processing Addendum, then Google does not share such data without customer authorisation or notification pursuant to Section 11 (Subprocessors) of the Cloud Data Processing Addendum. If logging data is Service Data under the Google Cloud Privacy Notice, then Google may only share such data in the scenarios listed in the "How we Share Service Data" section of the Google Cloud Privacy Notice.
With respect to monitoring, there is a lack of standardised monitoring interfaces across CSPs. Therefore, to leverage multiple CSPs, there should be a standardised monitoring interface provided across all services.	Ref 3.3.7	Is your organisation´s monitoring approach covering all your services? Please explain in comment field.	CSA CCM v4.0.5: - LOG-07	PARTIAL	For a list of Google Cloud services that provide audit logs, see Google services with audit logs. All Google Cloud services will eventually provide audit logs. (https://cloud.google.com/logging/docs/audit/services)
	Ref 3.3.8	Does your organisation´s Security Monitoring service provide an interface so that interchange between different platforms is possible (e.g. open standards)? Please provide the interchange protocols in the comment field.	CSA CCM v4.0.5: - DSC-01	YES	Customers can export Security Command Center data in JSON format with the Security Command Center dashboard or Security Command Center API. For more information, see the Exporting Security Command Center Data page here: https://cloud.google.com/security-command-center/docs/how-to-export-data
	Ref 3.3.9	Does your organisation provide a complete set of policies to achieve compliance against industry standards (e.g. CIS benchmarks) out of the box?	CSA CCM v4.0.5: - AIS-01	YES	Google Cloud provides security best practices to all customers to help configure their environments. (https://cloud.google.com/security/best-practices) Google Cloud - Externally provided (CIS): Google Cloud Foundational Benchmark checklists are made available by CIS. (https://ncp.nist.gov/checklist/870; https://www.cisecurity.org/benchmark/google_cloud_computing_platform)
	Ref 3.3.10	Does your organisation provide out of the box management of these policies?	CSA CCM v4.0.5: - AIS-01	YES	See response to Ref 3.3.9
Subchapter 3.4 Data Exfiltration and Customer Policy Enforcement					
Since data sharing is quite effortless to perform on the cloud, customers are interested in strictly controlled data sharing capabilities to prevent data exfiltration to unwanted locations.	Ref 3.4.1	Does your organisation provide a way to restrict data to be localised in a chosen region only and by doing so prevent data transfers taking place towards unwanted locations e.g. outside the EEA?	CSA CCM v4.0.5: - DSP-08	YES	Google provides customers with choices about where to store their data. Once a location is chosen, Google will not store the customer data outside of the chosen region(s). Customers 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 customers on Google Cloud Whitepaper. (https://services.google.com/fh/files/misc/googlecloud_european_commitments_whitepaper.pdf)
Hence, CSP should provide consistent visibility and control of all workloads and communication flow perimeters regardless of location, size, or architecture. This also applies to communication between CSP services and 'private endpoints', including the direction of data flow (ingress/egress).	Ref 3.4.2	Can your organisation provide the detailed data flows, both ingress (inbound) / egress (outbound), of each cloud service being used by the customers?	CSA CCM v4.0.5: - DSC-09 ff.	YES	Customers can take advantage of Network Topology, a visualization tool that shows the topology of customers' Virtual Private Cloud (VPC) networks, hybrid connectivity to and from their on-premises networks, connectivity to Google-managed services, and the associated metrics. Customers can also view metrics and details of network traffic to other Shared VPC networks and inter-region traffic. Network Topology combines configuration information with real-time operational data in a single view. With Network Topology, customers can collect real-time telemetry and configuration data from Google's infrastructure to visualize their resources. (https://cloud.google.com/network-intelligence-center/docs/network-topology/concepts/overview)
A CSP should also provide an effective set of KMSs to enable customers to assess security configurations at a global cloud control layer in line with their security frameworks and standards.	Ref 3.4.3	Does your organisation provide an effective set of KMSs to enable customers to assess security configurations at a centralized global cloud control layer in line with their security frameworks and standards?	CSA CCM v4.0.5: - CEK-06, 08, 10	YES	See responses to Refs 3.1.7 - 3.1.14

In addition, each configuration and policy defined for a cloud service by a customer should be automatically applied across all instances of that service run by that customer and be centrally monitored thereafter.	Ref 3.4.4	Does your organisation provide for each service an automated policy enforcement as configured by the customers so that it can be monitored and validated upon policy compliance?	CSA CCM v4.0.5	YES	Google Cloud Armor exports monitoring data from security policies to Cloud Monitoring. You can use monitoring metrics to check whether your policies are working as intended or to troubleshoot problems. (https://cloud.google.com/armor/docs/monitoring) Through the Security Command Center, Customers can identify security misconfigurations and compliance violations in their Google Cloud assets and resolve them by following actionable recommendations. (https://cloud.google.com/security-command-center)
Subchapter 3.5 Service Certifications and Evidence					
Certifications for cloud services assure an adequate level of security and therefore are one of the key requisites for all cloud users to rely upon. Hence, the services of a CSP should be independently certified by independent certification authority.	Ref 3.5.1	Can your organisation demonstrate or evidence the independent certifications provided by certified authority?	BSI C5:2020 PCI DSS CSA STAR ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 AICPA SSAE 18 ISAE 3402 type II: SOC2	YES	Google recognizes that customeres 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 customers: -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 - CSA STAR - BSI C5:2020 Customers can review Google's current certifications, including related evidences or reports, at any time. (https://cloud.google.com/security/compliance/offerings/#/) Customers can also access the compliance reports manager, which provides an easy, on-demand access to these critical compliance resources. (https://cloud.google.com/security/compliance/compliance-reports-manager)
The security certifications should at least include the de facto market standards for cloud technology , as well as further certifications that are specific to the financial industry.	Ref 3.5.2	Does your organisation certify cloud products and services, with de facto market standards for cloud technology certifications? If yes, please specify in the comment field which certifications you have granted for which products and services.	BSI C5:2020 PCI DSS CSA STAR ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 AICPA SSAE 18 ISAE 3402 type II: SOC2	YES	Google Cloud products regularly undergo independent verification of their security, privacy, and compliance controls, achieving certifications, attestations, and audit reports to demonstrate compliance. Google has also created resource documents and mappings for compliance support when formal certifications or attestations may not be required or applied. Details: https://cloud.google.com/security/compliance Reports: https://cloud.google.com/security/compliance/compliance-reports-manager
A CSP should disclose evidence of certifications upon request to the customer. Furthermore, a CSP should provide its customers with the ability to conduct their own audits on the CSP.	Ref 3.5.3	Can your organisation provide (annually if possible) evidence of certifications of the services being used by the customers, so that this can be validated in an own audit?	BSI C5:2020 PCI DSS CSA STAR ISO/IEC 27001:2013 ISO/IEC 27017:2015 ISO/IEC 27018:2019 AICPA SSAE 18 ISAE 3402 type II: SOC2	YES	See responses to Refs 3.5.1 and 3.5.2
Subchapter 3.6 Separation of Identities and Contacts					
In the event an FI's identity and contact information are identical, there's a possibility that their associated contexts may get mixed up. A CSP should therefore provide the measures to associate federated and non-federated identities with valid routable contact information (e.g., email addresses) to ensure notifications are successfully delivered to the user. More precisely, identity identifier and contact information should be separated but able to be grouped by identities. For example, if an identity cannot be routed for notifications, at least a valid and routable email address should be able to be associated and used to send any notifications to and from the CSP.	Ref 3.6.1	Does your organisation provide measures to associate federated and non-federated identities with valid routable contact information (e.g., email addresses), to ensure notifications are succesfully delivered to the users? Please provide the details in the comment field.	CSA CCM v4.0.5: - LOG-08	YES	Customers can update contact information for notifications through the Essential Contacts function within Resource Manager. Customers can include email addresses to receive notifications. (https://cloud.google.com/resource-manager/docs/managing-notification-contacts#add)

A CSP should provide specific communication channels for certain event types, such as critical data and service events, e.g., data breaches, security issues, or technical blockers. This should be provided, in addition to email by other channels that can be configured by the customer.	Ref 3.6.2	For specific (critical/sensitive) event types, does your organisation provide a separate communication channel (in addition to email) that can be configured by the customer? Please describe the details of a separate communication channel for communication of such critical/sensitive data in the comment field.	CSA CCM v4.0.5: - LOG-08	YES	Google notifies customers of data incidents promptly and without undue delay. Notification is provided to an email address designated by the customer. Customers can choose to use Essential Contacts: https://cloud.google.com/resource-manager/docs/managing-notification-contacts.. More information on Google's data incident response process is available in our Data incident response whitepaper and the Cloud Data Processing Addendum. (https://services.google.com/fh/files/misc/data_incident_response_2018.pdf; https://cloud.google.com/terms/data-processing-addendum) The Google Cloud Service Health Dashboard (https://status.cloud.google.com/) shows incidents that affect many customers. When a relevant Google Cloud product or service reports an issue in the dashboard, customers may also see an outage notice in the Google Cloud console. Customers can also choose to build integration to consume the information displayed on the dashboard programmatically e.g. through an RSS feed. The Google Cloud Support Center (https://support.cloud.google.com/portal/) displays known issues. This is the most comprehensive view of issues, and includes issues that affect fewer customers than are shown on the dashboard. Customers can create a support case from a posted incident on the known issue page so that they get regular updates. Google offers Threat Horizons intelligence reports to help keep your organization on top of the latest developments in the security landscape: https://cloud.google.com/security/gcat Google publishes bulletins that contain public security updates, vulnerabilities and known issues for certain Google Cloud Platform Services, via https://cloud.google.com/support/bulletins

Subchapter 3.7 Maturity of Data-in-Use Security

As of now, to achieve data-in-use security, the only generic and practical method in the industry is to rely on Trusted Execution Environments as part of the computing processors. This functionality is often referred to as Confidential Computing. This feature is only offered by some CSPs for a few selected services restricted to specific hardware specifications. To enable customers to protect their data during usage, the CSP should provide Confidential Computing or similar implementations as an option for a broad set of hardware configurations as well as backends of managed services.	Ref 3.7.1	Does your organisation provide Confidential Computing or similar implementations? Please provide the list of services that you offer which support Confidential Computing as well as details on how it is implemented.	CSA CCM v4.0.5	YES	Google offers the following Confidential Computing services: - Confidential Google Kubernetes Engine Nodes enforce the use of Confidential VM for all of your GKE nodes. (https://cloud.google.com/kubernetes-engine/docs/how-to/confidential-gke-nodes) - Dataproc Confidential Compute features Dataproc clusters that use Confidential VMs. (https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/confidential-compute) For more information on Google's Confidential Computing services see here: https://cloud.google.com/confidential-computing?hl=en.

Subchapter 3.8 Backup Functionality, High Availability, and Disaster Recovery

A CSP should provide a geo-redundant backup solution which is independent of the service's API enablement status. The backup functionality should support service independent storage locations and should not rely on 3rd parties. Also, the backup measure should be coherent with the shared responsibility model for the cloud service models for IaaS, PaaS, SaaS	Ref 3.8.1	Does your organisation provide a geo-redundant backup solution for all cloud service models (IaaS, PaaS, SaaS) which is independent of the service's API enablement status, and support service independent of storage locations and not rely on 3rd parties? Please elaborate your answer in the comment field.	ISO/IEC 27002:20013: - Chapter 5.29, 7.5 ISO/IEC 27002:2022: - Chapter 5.29, 7.5, 8.14 ISO/IEC 27018:2019: - Chapter 5.29, 7.5	YES	Google's geographically dispersed storage services provide replication to backup system software and data so that user data is written to at least two other clusters. A combination of synchronous and asynchronous replication methods are used. Google's highly available solution is discussed in the security whitepaper: https://cloud.google.com/security/overview/whitepaper. Google's global infrastructure is designed with the highest levels of performance and availability in mind. Google's SLAs contain our commitments regarding availability of the Services. They are available on the Google Cloud Platform Service Level Agreements page. https://cloud.google.com/terms/sla/ In addition, Google provides tools to help you manage and scale your networks. Refer to our Google Cloud Networking Products page for more information. For example: - Cloud Load Balancing provides scaling, high availability, and traffic management for your internet-facing and private applications. - Dedicated Interconnect is a high-performance option providing direct physical connections between your on-premises network and Google's network.

This functionality should be provided by all services storing customer data or service configurations and be manageable through a single interface.	Ref 3.8.2	Is your organisation´s backup solution provided for all services storing customer data or service configurations, and can it be managed through a single interface?	ISO/IEC 27002:2013: - Chapter 12.3 ISO/IEC 27002:2022: - Chapter 8.13 ISO/IEC 27018:2019: - Chapter 12.3	YES	Google's management console provides centralized management capabilities for the Google Cloud Backup and DR Service. From the management console, customers can manage backup/recovery appliances and perform day-to-day operations. Backup/recovery appliances allow replicating data between any two appliances. Mores specifically, from the management console, customers can: - Perform an at-a-glance, aggregated view of backup/recovery appliance health and resource utilization through the dashboard for all managed appliances. - Discover and manage applications using the Onboarding Wizard. - Manage backup/recovery appliances through the Manage tab, create organizations and assign resources, create roles, and create users and assign roles. In addition, customers create and manage storage pools. - Configure backup plans to define how long to retain the data. - Mount backup images of Compute Engine instances. - Monitor backup/recovery appliance health and system performance in real-time with the monitor. - View reports about jobs, backup plan compliance, resource utilization, and audit reports. https://cloud.google.com/backup-disaster-recovery/docs/concepts/introduction
For business continuity reasons, cloud services should be available in both High Availability and Disaster Recovery mode, so as not to create a single point of failure for FIs. Furthermore, if the CSP performs business continuity and resilience exercises affecting customers, they should be informed of the process and able to veto.	Ref 3.8.3	Are your organisation´s cloud services available in both High Availability and Disaster Recovery mode?	ISO/IEC 27001:2013: - Chapter 17.2 ISO/IEC 27002:2022: - Chapter 8.14 ISO/IEC 27018:2019: - Chapter 17	YES	Customers are also able to configure their Cloud Architecture to achieve HA and DR mode HA: Design a multi-zone architecture with failover for high availability Make your application resilient to zonal failures by architecting it to use pools of resources distributed across multiple zones, with data replication, load balancing and automated failover between zones. Run zonal replicas of every layer of the application stack, and eliminate all cross-zone dependencies in the architecture. https://cloud.google.com/architecture/framework/reliability/design-scale-high-availability#design_a_multi-zone_architecture_with_failover_for_high_availability DR: Replicate data across regions for disaster recovery Replicate or archive data to a remote region to enable disaster recovery in the event of a regional outage or data loss. When replication is used, recovery is quicker because storage systems in the remote region already have data that is almost up to date, aside from the possible loss of a small amount of data due to replication delay. When you use periodic archiving instead of continuous replication, disaster recovery involves restoring data from backups or archives in a new region. This procedure usually results in longer service downtime than activating a continuously updated database replica and could involve more data loss due to the time gap between consecutive backup operations. Whichever approach is used, the entire application stack must be redeployed and started up in the new region, and the service will be unavailable while this is happening. For a detailed discussion of disaster recovery concepts and techniques, see Architecting disaster recovery for cloud infrastructure outages. https://cloud.google.com/architecture/framework/reliability/design-scale-high-availability#replicate_data_across_regions_for_disaster_recovery
	Ref 3.8.4	Can customer choose to opt-out or are they able to veto when your business continuity and resilience exercises are expected to have a negative impact on customers' availability?	CSA CCM v4.0.5: - BCR-01 ff.	PARTIAL	Google's business continuity and resilience exercises are designed so that they do not impact customer Service availability.
Due to the central relevance of a KMS to provide cryptographic processes, a solution should be in place that enables CSP services to perform cryptographic tasks even when the main KMS is unavailable. This holds true especially for single region services.	Ref 3.8.5	Is your organisation´s KMS implemented with resilience in mind so that your cloud services continue to perform cryptographic tasks even when the main KMS is unavailable?	ISO/IEC 27002:2013: - Chapter 10.1 ISO/IEC 27002:2022: - Chapter 8.24 ISO/IEC 27018:2019: - Chapter 10.1	YES	KMS implementation is designed from the ground up to be resilient to outages due to their regional distribution and the ability to perform cryptographic tasks even when the entire region or zone is down.

Hence, a KMS should have a multi-region setup allowing the provisioning of multiple different keys to a specific service to overcome the risk of unavailability of an otherwise single point of failure KMS service.	Ref 3.8.6	Is your organisation´s KMS implemented as a multi-region setup to overcome the risk of unavailability of an otherwise single point of failure?	ISO/IEC 27002:2013: - Chapter 10.1 ISO/IEC 27002:2022: - Chapter 8.24 ISO/IEC 27018:2019: - Chapter 10.1	YES	Customers are able to select locations that are made up of Multi-regions when configuring Cloud KMS. See link below for further details https://cloud.google.com/kms/docs/locations
While multi-regional services enable a geo-redundant setup, the set of single regions should be clearly defined for the multi-region. A CSP's customer should be able to customize a multi-region or select of several pre-defined multi-regions in the same geographical region.	Ref 3.8.7	Is the customer able to customize a multi-region or select out of several pre-defined multi-regions in the same geographical region?	ISO/IEC 27001:2013	YES	See response to Ref 3.8.6

Subchapter 3.9 Software Supply Chain Transparency

Customer assets such as applications run on various underlying infrastructure managed by the CSP. This consists also of software, such as operating systems and management tools. Since the layer below the customer's view is only available to the CSP, the responsibility for this software stack is with the CSP. Therefore, a CSP should provide methods such as auditing processes and security evidence in order to provide transparency on its underlying software supply chain towards the customer. This helps FIs to comply with EBA requirements , where applicable CSP should provide detailed information to deliver the service chain.	Ref 3.9.1	To be able to comply with EBA-requirement, can your organisation provide methods such as auditing processes and security evidence in order to provide transparency on underlying software supply chain towards the customer?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 67-80	YES	Google centralizes control of our software supply chain and actively secures each step of the end-to-end process. We start by maintaining separate secured copies of the source code for our dependencies and perform our own vulnerability scanning. Most of our source code is stored in a central monolithic repository, which enables employees to check code into a single location. The Google codebase simplifies source code management, in particular management of our dependencies on third-party code. A monolithic codebase also allows for the enforcement of a single choke point for code reviews. We continuously fuzz 550 of the most commonly-used open source projects. We then manage an end-to-end build, deploy, and distribution process that includes integrated integrity, provenance, and security checks. In addition: -Based on our internal security practices, Binary Authorization for Borg, we have created the SLSA framework to enable organizations to assess the maturity of their software supply chain security and understand key steps to progress to the next level. SLSA lays out an actionable path for organizations to increase their overall software supply-chain security by providing step-by-step guidelines and practical goals for protecting source and build system integrity. The SLSA framework addresses a limitation of Software Bills of Materials (SBOMs), which on their own do not provide sufficient information about integrity and provenance. -Assured OSS allows enterprise customers to directly benefit from the in-depth, end-to-end security capabilities and practices we apply to our own OSS portfolio by providing access to the same OSS packages that Google depends on.

Subchapter 3.10 IAM and Privilege Escalation

Assets, such as data of customers, reside in CSP's services and access to these are controlled via Identity & Access Management (IAM). This is a core feature and should be a foundation to build upon, where user access rules are defined, controlled and managed solely by the cloud customers. However, if this is not implemented correctly, the risk of privilege escalation may emerge (with associated risks such as identity theft and data leakage), resulting in higher privileges than users should have in the first place. It should not be possible to gain access to a system without proper IAM settings. The CSP is responsible to deliver a sound IAM implementation across all its services to enable the definition, enforcement, and maintenance of IAM roles and permissions. This should result in a managed infrastructure, which is only accessible via a secured IAM system.	Ref 3.10.1	Does your organisation provide an integrated Identity & Access Management (IAM) service that allows cloud customers to configure and solely manage their user population and access? Please provide the details in the comment field.	ISO/IEC 27002:2013: - Chapter 9.2 ISO/IEC 27002:2022: - Chapter 8.24 ISO/IEC 27018:2019: - Chapter 5.2, 5.3, 5.18, 8.5 CSA CCM v4.0.5: - BCR-01 ff	YES	Customers can use IAM to manage access within their system. IAM lets customers adopt the security principle of least privilege, which states that nobody should have more permissions than they actually need. With IAM, customers manage access control by defining who (identity) has what access (role) for which resource. For example, Compute Engine virtual machine instances, Google Kubernetes Engine (GKE) clusters, and Cloud Storage buckets are all Google Cloud resources. The organizations, folders, and projects that you use to organize your resources are also resources. In IAM, permission to access a resource isn't granted directly to the end user. Instead, permissions are grouped into roles, and roles are granted to authenticated principals. An allow policy, also known as an IAM policy, defines and enforces what roles are granted to which principals. Each allow policy is attached to a resource. When an authenticated principal attempts to access a resource, IAM checks the resource's allow policy to determine whether the action is permitted. https://cloud.google.com/iam/docs/overview
	Ref 3.10.2	Is your organisation´s Identity & Access Management (IAM) service implemented in such a way that access control is enforced and users are not able to bypass it (e.g. potentially gain access to a system without proper IAM settings)? Please provide the details in the comment field.	ISO/IEC 27002:2013: - Chapter 9.2 ISO/IEC 27002:2022: - Chapter 8.24 ISO/IEC 27018:2019: - Chapter 5.2, 5.3, 5.18, 8.5 CSA CCM v4.0.5: - BCR-01 ff.	YES	See response to Ref 3.10.1
	Ref 3.10.3	Can your organisation´s Identity & Access Management (IAM) service prevent user privilege escalation ? Please provide the details in the comment field.	CSA CCM v4.0.5: - IAM-01 ff.	YES	See response to Ref 3.10.1

Subchapter 3.11 Workload Isolation

Various workloads of different customers will reside at the same CSP. Therefore, it should never be possible to access any other customer's assets without explicit consent. This includes data, software, infrastructure, and containers or virtual machines.	Ref 3.11.1	Are customer's cloud deployment fully isolated in such a way that it is not possible to access any other customer's assets without explicit consent/approval? This includes data, software, infrastructure, and containers or virtual machines.	CSA CCM v4.0.5: - IVS-06	YES	Google's infrastructure is designed to logically isolate each customer's data from the data of other customers and users, even when it's stored on the same physical server. For more information, see our Google security overview paper. (https://cloud.google.com/docs/security/overview/whitepaper)
The CSP should deliver evidence of periodic review of isolation controls that are effective including corrective measures. Updating systems and publishing reports will increase transparency.	Ref 3.11.2	Can your organisation demonstrate or provide evidence of periodic reviews of isolation controls, that they are effective and that - if necessary - corrective measures were taken?	CSA CCM v4.0.5: - IVS-05 ff.	YES	Isolation controls are tested as part of Google's compliance program. More information is available on the FedRAMP Compliance website - https://cloud.google.com/security/compliance/fedramp

Subchapter 3.12 Malware Defence

Due to the variety of services offered by a CSP, this enables different entry points for malware, such as ransomware. For the parts of the shared responsibility model the CSP is responsible for, the malware needs to be kept away from customer systems while at the same time the customers should have the possibility to use specialized tools to prevent, detect, and mitigate malware impact. Thus, the CSP should provide a threat intelligence to isolate threats without disruption and alert the customer with the option to clean infected systems.	Ref 3.12.1	Does your organisation have a threat detection service that can protect against threats to avoid disruption and alert the customer with the option to clean infected systems? Please provide the details in the comment field.	CSA CCM v4.0.5: - TVM-01,02	YES	Event Threat Detection is a built-in service for the Security Command Center Premium tier that continuously monitors customer's organization and identifies threats within their systems in near-real time. Event Threat Detection is regularly updated with new detectors to identify emerging threats at cloud scale. How Event Threat Detection works Event Threat Detection monitors customer's organization's Cloud Logging stream and Google Workspace Logs, and consumes logs for their projects as they become available. Cloud Logging contains log entries of API calls and other actions that create, read, or modify the configuration or metadata of your resources. Log entries contain status and event information that Event Threat Detection uses to quickly detect threats. Event Threat Detection applies detection logic and proprietary threat intelligence, including tripwire indicator matching, windowed profiling, advanced profiling, machine learning, and anomaly detection, to identify threats in near-real time. When Event Threat Detection detects a threat, it writes a finding to Security Command Center and to a Cloud Logging project. From Cloud Logging and Google Workspace logging, customers can export findings to other systems with Pub/Sub and process them with Cloud Functions. https://cloud.google.com/security-command-center/docs/concepts-event-threat-detection-overview
For the parts of the shared responsibility model the customer is responsible for, the CSP should offer tools to prevent misuse and infection of its services.	Ref 3.12.2	Does your organisation offer tools to the customer to prevent misuse and malware infection of cloud services used by the customers? Please provide the details in the comment field.	ISO/IEC 27002:2013: - Chapter 12.2 ISO/IEC 27002:2022: - Chapter 8.7 ISO/IEC 27018:2019: - Chapter 12.2	YES	See response to Ref 3.12.1

Chapter 4 - Governance and Regulation

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	Ref. ID	Questions related to reg. reference	Reg. reference	Offered / fulfilled by CSPs	Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.
Subchapter 4.1 Control measures on Outsourced Services					
To control outsourced services and systems implemented on cloud platforms, the following information on outsourced services should be made available to the customer on near real-time basis (case related) or via adequate alerts with defined and transparent thresholds: - Information on geographical/regional aspects and the provider's landscape including their data center location - Defined, implemented and tested contingency measures for the used services and infrastructure - Adequate contingency solutions to allow instant action to keep the service running or to fix problems - Conditions upon which contingency measures can be justified when it comes to 3rd country data transfer - Contingency measures that include or risk 3rd country data transfer should be made transparent in standard contractual clauses - Supplied information should include the CSP supply chain and sub-outsourcing, where applicable.	Ref 4.1.1	In general, does your organisation provide information or alerts on the availablity of the used services at least on a near real-time basis to monitor the performance of the outsourced arrangements? Please specify in comment field.	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 74, 75, 100 ff.	YES	Customers can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services, including: - The Google Cloud Service Health Dashboard (https://status.cloud.google.com/). More information about the the Service Health Dashboard is available at https://cloud.google.com/support/docs/dashboard. This includes what type of status information is available on the Dashboard and information about how customers can build integration to consume the data displaed on the Dashboard programmatically. - The Google Cloud Support Center (https://support.cloud.google.com/portal/) displays known issues. This is the most comprehensive view of issues, and includes issues that affect fewer customers than are shown on the dashboard. Customers can create a support case from a posted incident on the known issue page so that they get regular updates. - Google Cloud Operations: an integrated monitoring, logging, and diagnostics hosted solution that helps customers gain insight into their applications that run on Google Cloud, including availability and uptime of the services. https://cloud.google.com/monitoring/
	Ref 4.1.2	Does your organisation provide contingency measures for the used services on a near times basis to monitor the performance of the outsourced arrangements, according to the EBA/GL/2019/02 (Outsourcing)?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 74, 75, 100 ff.	YES	Google recognizes that resilience is a key focus for regulated entities and supervisory authorities. Our Strengthening operational resilience in financial services by migrating to Google Cloud whitepaper discusses the continuing importance of operational resilience to the financial services sector, and the role that a well-executed migration to Google Cloud can play in strengthening it. Our Infrastructure design for availability and resilience whitepaper explains how Google Cloud builds resilience and availability into our core infrastructure and services, from design through operations. We also explore the shared fate model between Google and our customers—how customers can build on top of the core services we provide to gain the level of availability and resilience they need to run their businesses and meet their regulatory and compliance obligations. Google implements business continuity plans for our Services, reviews and tests it at least annually and ensures it remains current with industry standards. In addition to testing our own environments, Google also provides a number of tools and resources that enable firms to independently test their Google Cloud deployments. - Google provides information about how customers can use our Services in their own business contingency planning in our Disaster Recovery Planning Guide. https://cloud.google. com/solutions/dr-scenarios-planning- guide . This includes information about how customers can achieve their own reliability outcomes for their applications. -Our Disaster Recovery Scenarios for Data (https://cloud.google.com/architecture/dr-scenarios-for-data) and Disaster Recovery for Applications (https://cloud.google.com/architecture/dr-scenarios-for-applications) articles provide information about common disaster scenarios for backing up and recovering data and for applications, respectively.

Ref 4.1.3	Does your organisation break down availabilty information and contingency measures to services and regions/zones to monitor the performance of the outsourced arrangements?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 74, 75, 100 ff.	YES	The Google Cloud Service Health Dashboard (https://status.cloud.google.com/) provides status information by services and by region.
Ref 4.1.4	Does your organisation inform about 3rd country data transfer to monitor the security & data protection of outsourced services?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 74, 75, 78, 83	YES	Data transfers are addressed in the Cloud Data Processing Addendum (https://cloud.google.com/terms/data-processing-addendum) To provide you with a fast, reliable, robust and resilient service, Google Cloud 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. -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. 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 customers on Google Cloud Whitepaper.
Ref 4.1.5	Is the above mentioned information provisioning referenced in your organisation´s standard contractual clauses?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75, 100 ff.	YES	Google Cloud's Standard Contractual Clauses are available in the Cloud Data Processing Addendum (https://cloud.google.com/terms/data-processing-addendum) More information on Google Cloud's approach to the EU standard contractual clauses can be found here: https://services.google.com/fh/files/misc/gc_new_eu_scc.pdf

Subchapter 4.2 CSP should provide Information for a sound 3rd Party Risk Management

For a sound governance of 3rd Party Risk Management, CSPs should provide FIs with the following information for the used cloud services and infrastructure, that is deemed to be sufficient for an FI specific Business Continuity and Disaster Recovery Plans:
- Overview of cloud services including a detailed supply-chain service mapping of underlying dependent sub-contractors or sub-hosting services
- Supply-chain information detailing the roles and responsibilities of the underlying sub-contractors for the related cloud services
- Supply-chain information detailing the dataflow, data exchange and data location/region between the CSP and each sub-contractor for the related cloud services.

Ref 4.2.1	Does your organisation provide a present list of all sub-contractors relevant for FI's cloud usage to control and manage the risk of outsourced arrangement?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 76 ff.	YES	Google Cloud publishes a list of subcontractors that access and process customer data (i.e. subprocessors) for Google Cloud at https://cloud.google.com/terms/subprocessors In addition, upon request, Google Cloud provides regulated customers information about subcontractors that do not access or process customer data.
Ref 4.2.2	Does your organisation inform about changes in sub-contractors to control and manage the risk of outsourced arrangement?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 76 ff.	YES	Google Cloud provides advance notice of changes to our subcontractors. Notification is provided to an email address designated by the customer. Customers can choose to use Essential Contacts: https://cloud.google.com/resource-manager/docs/managing-notification-contacts Subcontractor notifications are sent to the "Legal" category.
Ref 4.2.3	Does your organisation provide the list of services managed by the sub contractors/sub-processors and which kind of data access are processed by them? Please provide a list or link in the comment field.	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 76 ff.	YES	See response to Ref 4.2.1. These lists describe the services provided by subcontractors/subprocessors and their data processing activities.
Ref 4.2.4	Does your organisation inform about the location of customer data at rest, in transport (only if managed by the CSP) and in use (especially when subcontractors are part of the service operation) to control and manage the risk of outsourced arrangement?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 76 ff.	YES	Information about the location of Google's facilities and where individual Google Cloud services can be deployed is available on our Global Locations page. Google Cloud's subprocessor list (https://cloud.google.com/terms/subprocessors) also indicates the country where processing is performed.

	Ref 4.2.5	Does your organisation provide a due diligence for each of the sub contactors/sub-processors?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 79	YES	Google requires our subcontractors/subprocessors to meet the same high standards that we do. Before engaging a subcontractor/subprocessor, Google conducts an assessment considering the risks related to the subcontractor/subprocessor and the function to be subcontracted to confirm that the subcontractor/subprocessor is suitable. To assist regulated customers with their own due diligence, Google will provide all the information required in the outsourcing register for each of our subcontractors.

Subchapter 4.3 Exit Strategy Requirements

The European Banking Authority (EBA) guidelines on outsourcing arrangements require FIs as part of their risk assessment to have an exit strategy in place when outsourcing any "Critical / Important function" to CSPs. This is to cover relevant exit triggering events, e.g. bankruptcy of CSP, sanctions, or a changing legal environment. Relevant exit triggering events can be observed, and the occurrence anticipated. On that basis along with empirical data from such events, an exit and migration time slot can be defined to exit a cloud platform and migrate the bank critical service. We ask to outline feasible time slots for exit plan execution that is connected to the materiality assessment of the outsourcing.	Ref 4.3.1	Does your organisation duly inform about discontinuation of used services or contractual arrangements to prevent an unexpected interrupt of outsourced arrangements? Please specify the days in advance, like e.g. 180 days in the comment field.	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 42, 76 ff., 106	YES	Google recognizes that our approach to change management is important to your own change management processes. 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.
	Ref 4.3.2	Does your organisation offer a dedicated post-termination period?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 42, 76 ff., 106	YES	Google recognizes that regulated entities need sufficient time to exit our services (including to transfer services to another service provider). 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.

Subchapter 4.4 CSP Audits and Oversight

We propose simplifications in audit procedures insofar as the cloud service offerings are not checked by every FI, but centrally at the CSP. We want to facilitate the implementation of regulatory requirements at CSPs: Collaborative audits organised by the financial industry should become a generally accepted approach by CSPs and free of charge. Different institutions form a collaborative team to audit one specific CSP. The audit results can be regarded valid within the respective individual institution. Collaborative audits are already supported by the EBA Guidelines on Outsourcing Arrangements (Art. 13.3.91.a). Currently CSPs are audited by European supervision along onsite inspections at Financial Institutes. On that basis a particular CSP is audited multiple times whenever Financial Institutes as CSP customers are inspected on their public outsourcing activities. National and European supervision are asked to form collaborative audit teams to audit CSPs across countries and for all Financial Institutions being customers of a CSP. Such an approach could improve consistency of observations, and additionally be more efficient. In addition, we point out that the systemic risk of the entire industry using CSP cannot be managed by individual institutions. However, the institutions specific cloud adoption is still inspected individually and resulting observations are assigned to the respective institution.	4.4.1	Does your organisation support pooled audits performed by FIs themselves to use audit resources more efficiently and to decrease organisational burden?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 91	YES	Google recognizes the benefits of pooled audits. We would be happy to discuss this with regulated entities. For more information about Google's approach to pooled audits, refer to our 'Verifying the security and privacy controls of Google Cloud: 2021 CCAG customer pooled audit' and 'Earning customer trust through a pandemic: delivering our 2020 CCAG pooled audit' blog posts.

Chapter 5 - Contractual Clauses

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	Ref. ID	Questions related to reg. reference	Reg. reference	Offered / fulfilled by CSPs	Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.
Subchapter 5.1 Audit Rights for Customers					
To meet industry's obligations to audit, audit rights to data centers and its services, Customers Audit Rights should be granted per standard contractual clauses. There is also a need to audit the relevant infrastructure on a regular basis. With referance to the requirements set out in the EBAs Guidelines on Outsourcing Arrangments (EBA/GL/2019/02), the written outsourcing arrangements should at least include the unrestricted right to inspect and audit the service provider especially with regards to the critical or important outsourced function. This would include but not be restricted to for instance data centers. Therefore, you are kindly asked to provide answers to the following questions.	Ref 5.1.1	Does your organisation offer rights to your customers, their auditors, and competent authorities without restricting them to inspect and audit your services with regards to the functions and services outsourced to your institution in accordanace with the written outsourcing arrangement?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.p, 85.ff	YES	Google grants information, audit and access rights to our customers, competent authorities, and both their appointees. This includes access to Google's premises used to provide the Services to conduct an on-site audit. Nothing in our contract is intended to restrict, limit or impede the auditing party's ability to audit our services effectively. Google Cloud Financial Services Contract ref: Regulator Information, Audit and Access, Customer Information, Audit and Access
	Ref 5.1.2	Does your organisation grant by the written outsourcing agreement: a. full access to all relevant business premises (e.g. head offices and operation centers), 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 service provider's external auditors ('access and information rights'); and b. unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 87	YES	See response to Ref 5.1.1.
	Ref 5.1.3	Does your service arrangement make third party certifications, including related evidences or reports, available to the customer?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 91.b	YES	Customers can review Google's current certifications at any time. (https://cloud.google.com/security/compliance/offerings/#/) Customers can also access the compliance reports manager, which provides an easy, on-demand access to these critical compliance resources. (https://cloud.google.com/security/compliance/compliance-reports-manager) Google Cloud Financial Services Contract ref: Certifications and Audit Reports
	Ref 5.1.4	Does your service arrangement make third party audits or internal audit reports available to the customer?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 91.b	YES	See response to Ref 5.1.3.
	Ref 5.1.5	Does your organisation provide the scope of certifications or audit reports which cover the systems (e.g. processes, applications, infrastructure, data centers, etc.) and key controls identified by the Financial Institutions?	EBA/GL/2019/02 (Outsourcing): - Chap. Para. 93.b	YES	See response to Ref 5.1.3. Refer to the relevant certification or audit report for information about in scope systems. Google Cloud Financial Services Contract ref: Certifications and Audit Reports
	Ref 5.1.6	Does your organisation provide the certifications and evidences or reports on a regularly basis?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 93.c	YES	See response to Ref 5.1.3. Google is audited at least once a year for each audited framework. Customers can review Google's current certifications and audit reports at any time. Google Cloud Financial Services Contract ref: Certifications and Audit Reports
	Ref 5.1.7	Does your organisation ensure that key systems and controls will be covered in future versions of your certification or audit report?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 93.d	YES	See response to Ref 5.1.3. 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. Google Cloud Financial Services Contract ref: Certifications and Audit Reports

	Ref 5.1.8	Does your organisation grant the right by contract to request expansion of the scope of the certifications or audit reports or relevant systems and controls?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 93.g	YES	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, Google grants regulated entities have the contractual right to request an expansion of the scope. Google Cloud Financial Services Contract ref: Certifications and Audit Reports
	Ref 5.1.9	Does your organisation grant the contractual right to perform individual audits at banks' discretion with regard to the outsourcing of critical or important functions?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 93.h	YES	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) information, audit and access rights. 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. Google Cloud Financial Services Contract ref: Customer Information, Audit and Access
	Ref 5.1.10	Does your service arrangement permit pooled audits?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 91 a	YES	Google recognizes the benefits of pooled audits. We would be happy to discuss this with regulated entities. For more information about Google's approach to pooled audits, refer to our 'Verifying the security and privacy controls of Google Cloud: 2021 CCAG customer pooled audit' and 'Earning customer trust through a pandemic: delivering our 2020 CCAG pooled audit' blog posts.
	Ref 5.1.11	Concerning pooled audits, does your organisation provide full visibility on internal CSP procedures and documentation in a confidential way to permit to the EU legal entities to satisfy the inspection activities?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 91.b	YES	Google has developed secure processes and tools to share information about our procedures and documentation in a confidential manner during audits. For more information about Google's approach to pooled audits, refer to our 'Verifying the security and privacy controls of Google Cloud: 2021 CCAG customer pooled audit' and 'Earning customer trust through a pandemic: delivering our 2020 CCAG pooled audit' blog posts.
Summary	Ref 5.1.12	Has your organisation regulated all the above requirements in the standard contract or a specific contractual amendment?		YES	This addressed in Google Cloud Financial Services Contract Google Cloud Financial Services Contract ref: Regulator Information, Audit and Access, Customer Information, Audit and Access, Certifications and Audit Reports

Subchapter 5.2 Sub-Outsourcing

In accordance with the EBA "Guidelines on Outsourcing Arrangements" the CSP provides information regarding sub outsourcing at any time without limitations.	Ref 5.2.1	Does your organisation provide information such as a registry of sub-contractors and their potential third-country transfer of data to your customers to ensure that any risks can be identified and mitigated?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 55.g, 67	YES	Google Cloud publishes a list of subcontractors that access and process customer data (i.e. subprocessors) for Google Cloud at https://cloud.google.com/terms/subprocessors. In addition, upon request, Google Cloud provides regulated entities information about subcontractors that do not access or process customer data. These materials include information about service location and the countries where processing takes place. Google Cloud Financial Services Contract ref: Google Subcontractors; Subprocessors (Cloud Data Processing Addendum)
	Ref 5.2.2	For sub-outsourcing does your organisation a. in the sub-outsourcing arrangement oversee and ensure that all contractual obligations between your institution and the customer are continuously met if sub-outsourcing takes place? and b. does your organisation ensure that the same contractual and regulatory requirements stipulated in your service arrangement also apply to these arrangements including the requirements to grant rights of access and audit in accordance with Ref 5.1.1?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 79	YES	Google requires our subcontractors to meet the same high standards that we do. Google will oversee the performance of all subcontracted obligations and ensure our subcontractors comply with our contract with you. Google recognizes that chain-outsourcing must not reduce the regulated entity's or the supervisory authority's ability to supervise the relevant activity. To preserve this, Google will ensure our subcontractors comply with the information, audit and access rights we provide to regulated entities and supervisory authorities. Google Cloud Financial Services Contract ref: Google Subcontractors; Subprocessors (Cloud Data Processing Addendum)

	Ref 5.2.3	Does your organisation provide any information during the due diligence phase to support the Financial Institute to evaluate the potential risk?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 69	YES	Google provides all the information required in the outsourcing register for each of our subcontractors. This information is available to regulated entities when they perform due diligence of Google Cloud's services. In addition, Google provide advance notice before we engaged a new subcontractor or change the function of an existing subcontractor. This notice also contains the information required in the outsourcing register for the relevant subcontractor. Google Cloud Financial Services Contract ref: Google Subcontractors; Subprocessors (Cloud Data Processing Addendum)
In addition and following our experiences, we regard a prenotification of minimum 90 days as being adequate to show all changes with the right of consultation.	Ref 5.2.4	Does your organisation notify your customers in advance regarding potential changes to the outsourcing arrangement or the service provided including sub-outsourcings and the right of consultation?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 42.d.ii, 44.f, 78.e	YES	Regulated entities 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 Cloud Financial Services Contract ref: Google Subcontractors; Subprocessors (Cloud Data Processing Addendum)
The CSP should ensure that the objections of FIs are examined favourably.	Ref 5.2.5	Does your organisation ensure that objections to the suboutsourcing by the FI are duly taken into account?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 78.f	YES	Google will discuss a regulated entity's concerns with a subcontractor change and consider appropriate ways to address them. To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will give regulated entities the ability to terminate if they have concerns about a new subcontractor. Google Cloud Financial Services Contract ref: Google Subcontractors; Subprocessors (Cloud Data Processing Addendum)
	Ref 5.2.6	Does your organisation inform customers in advance to perform a risk assessment? Please specify how many days in advance in the comment field.	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 44.f, 78.d, 78.f	YES	See response to Ref 5.2.5. Google offers at least 90 days' notice. Google Cloud Financial Services Contract ref: Google Subcontractors; Subprocessors (Cloud Data Processing Addendum)
	Ref 5.2.7	In case that your organisation does not grant the right to object, do you offer termination support in case of undue sub-outsourcing?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 78.d, 78.f	YES	To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will give regulated entities the ability to terminate if they have concerns about a new subcontractor. Google Cloud Financial Services Contract ref: Google Subcontractors; Subprocessors (Cloud Data Processing Addendum)
In the event of use of unsuitable subcontractors, the FI should be granted a special right of termination including termination support.	Ref 5.2.8	Does your organisation offer the right to terminate the contract in case of undue sub-outsourcing or in any case by the customer?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 78.g	YES	To enable regulated entities to retain oversight of any subcontracting and provide choices about the services regulated entities use, Google will give regulated entities the ability to terminate if Google does not provide the agreed notice. In addition, regulated entities can elect to terminate our contract for convenience for any reason with advance notice. Google Cloud Financial Services Contract ref: Google Subcontractors; Subprocessors (Cloud Data Processing Addendum), Term and Termination
	Ref 5.2.9	Does your organisation offer a transition period when the customer is forced to terminate the contract?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 99.b	YES	Google recognizes that regulated entities need to be able to exit our Services without undue disruption to their business, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of their service to their own clients. To help regulated entities achieve this, upon request, Google will continue to provide the Services for 12 months beyond the expiry or termination of the contract. Google Cloud Financial Services Contract ref: Transition Term
Summary	Ref 5.2.10	Has your organisation regulated all the above requirements in the standard contract or a specific contractual amendment?		YES	This addressed in Google Cloud Financial Services Contract Google Cloud Financial Services Contract ref: Google Subcontractors; Subprocessors (Cloud Data Processing Addendum); Transition Term

Subchapter 5.3 Embedded URLs in Contracts and Service Level Agreements

In Accordance with EBA Guidelines on Outsourcing, CSPs should provide clear financial obligations within the contract.	Ref 5.3.1	Does your organisation provide clear financial obligations by a written contract for your services, including clear rules on price increases according to periods with price guarantee/fixed price.	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.d	YES	Prices and fee information are addressed in the contract. This information is also publicly available on our SKUs page. Refer to our Pricing page for more information. Google notifies customers at least 30 days in advance of any Price increases. Google also offers committed use discounts and is happy to discuss a regulated entities specific cost/pricing needs. Google Cloud Financial Services Contract ref: Payment Terms
Unilateral changes by the CSPs using embedded URLs in contract should not affect the agreed Terms and Conditions during the contract period. This prevents a sudden increase in cost which can occur after offering an attractive price model for the initial contract phase.	Ref 5.3.2	Does your organisation provide stable Terms and Conditions for your services for an agreed contract period?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.i DORA: - Art. 25.9	YES	As services and technology change, Google may update certain terms at URLs that apply to all our customers. Any updates must meet strict criteria. For example, they must not result in a material degradation of the overall security of the services or have a material adverse impact on your existing rights. Beyond these limited updates, any contract changes must be made in writing and signed by both parties. Google Cloud Financial Services Contract ref: Changes to Terms; Amendments
Likewise, the CSP should only change the service in a way that guarantees all cloud customers at least equal or improved services in terms of function, security, technology and data protection,	Ref 5.3.3	Does your organisation provide backward compatibility for any service change?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 DORA: - Art. 25.9	PARTIAL	Google notifies customers at least 12 months before significantly modifying a Customer-facing Google API in a backwards-incompatible manner. See our Compatibility page for more information. Google Cloud Financial Services Contract ref: Changes to Services
	Ref 5.3.4	In the event of a service change(s), is there a gurantee that are overall security standards and data protection are kept at least at the previous level?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 DORA: - Art. 25.9	YES	Google will not make updates to the Services that result in a material reduction of the functionality, performance, availability, or security of the Services. Google Cloud Financial Services Contract ref: Changes to Services
or that a change or termination of the service will be announced with a prenotification period and without undue delay.	Ref 5.3.5	Does your organisation offer prenotification periodes in case of major changes or termination of services? Please provide more details in the comment field.	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107 DORA: - Art. 25.9	YES	Google notifies customers at least 12 months before discontinuing any Service (or associated material functionality) unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality. Google notifies customers at least 12 months before significantly modifying a Customer-facing Google API in a backwards-incompatible manner. Google Cloud Financial Services Contract ref: Changes to Services
In addition to availability, the Service Level Agreements (SLA) should also include performance metrics and reporting thereof. Both values require permanent monitoring and automation for reporting deviations.	Ref 5.3.6	Does your SLA include performance metrics and permanent monitoring and reporting?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.h, 75.i, 75.p, 82, 85, 87, 88, 90, 91b, 92, 93	YES	The SLAs provide measurable performance standards for the services and are available on our Google Cloud Platform Service Level Agreements page. Customers can monitor Google's performance of the Services (including the SLAs) on an ongoing basis using the functionality of the Services, including: - The Google Cloud Service Health Dashboard (https://status.cloud.google.com/) - Google Cloud Operations: an integrated monitoring, logging, and diagnostics hosted solution that helps customers gain insight into their applications that run on Google Cloud, including availability and uptime of the services. (https://cloud.google.com/monitoring/) Google Cloud Financial Services Contract ref: Services, Ongoing Performance Monitoring

The CSP should offer additional communication channels to transmit critical event and service level information (e.g. on data breaches, penetration test findings, logfiles for problem analysis) besides email and a definition of which channels are to be used for different types of information, e.g., via phone. All such events should be available to the customer regardless if the CSP has concluded that the customer is impacted or not. The customer must have the possibility to assess impact and not only rely on the CSP impact analysis.	Ref 5.3.7	Does your organisation offer dedicated communication channels and competent contacts for critical events, breaches, penetration tests and logfile issues?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.j, 98, 92	YES	Google offers a variety of support services and channels: https://cloud.google.com/support Customers can select the best service for their needs. Google makes information about developments that materially impact Google's ability to perform the Services in accordance with the SLAs available to customers. Google provides this information via the Google Cloud Service Health Dashboard, the Google Cloud Support Center or a support case. More information is available at our Incidents & the Google Cloud dashboard page. Google notifies customers via email of data incidents promptly and without undue delay. Notification is provided to an email address designated by the customer. Customers can choose to use Essential Contacts: https://cloud.google.com/resource-manager/docs/managing-notification-contacts More information on Google's data incident response process is available in our Data incident response whitepaper. Google engages a qualified and independent third party to conduct penetration testing of the Services. More information is available here. Regulated entities may review a report of the results of this penetration testing on request. Google Cloud Financial Services Contract ref: Technical Support; Significant Developments; Data Incidents (Cloud Data Processing Addendum), Customer Penetration Testing
	Ref 5.3.8	Does your organisation inform the customer about events in any case, not only if the customer is impacted?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.j, 85, 87, 88	YES	The Google Cloud Service Health Dashboard (https://status.cloud.google.com) shows incidents that affect many customers. When a relevant Google Cloud product or service reports an issue in the dashboard, customers may also see an outage notice in the Google Cloud console. Customers can also choose to build integration to consume the information displayed on the dashboard programmatically e.g. through an RSS feed. The Google Cloud Support Center (https://support.cloud.google.com/portal/) displays known issues. This is the most comprehensive view of issues, and includes issues that affect fewer customers than are shown on the dashboard. Customers can create a support case from a posted incident on the known issue page so that they get regular updates. Google offers Threat Horizons intelligence reports to help keep your organization on top of the latest developments in the security landscape: https://cloud.google.com/security/gcat Google publishes bulletins that contain public security updates, vulnerabilities and known issues for certain Google Cloud Platform Services, via https://cloud.google.com/support/bulletins
	Ref 5.3.9	Does your organisation offer Financial Institutions impact analyses in addition to your own?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.h, 75.i, 75.p, 93.g	YES	See response to Ref 5.3.7 and Ref 5.3.8. Customers can use the information provided by Google and information available via the Service to perform their own impact analyses. In addition, Google offers threat briefings, Threat Horizons intelligence reports, preparedness drills, incident support, and rapid response engagements in order to keep your organization on top of the latest developments in the security landscape: https://cloud.google.com/security/gcat Customers can perform penetration testing of the Services at any time without Google's prior approval. Google Cloud Financial Services Contract ref: Customer Penetration Testing
All terms, changes, and level of information should apply without exception to all consumers and not only to individual consumers.	Ref 5.3.10	Does your organisation state all terms/prenotification periods, communication channels tests etc. in a standard contract or a standard FSA?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 74	YES	Refer to your Google Cloud Financial Services Contract. Google Cloud Financial Services Contract ref: Technical Support; Significant Developments; Data Incidents (Cloud Data Processing Addendum)
Any changes to product terms (incl. FSA, DPA and SLA) should be highlighted on paragraph level in order to facilitate FI identification of the exact change and subsequent impact analysis. Documentation of changes should be logged by the CSP to allow for back-tracking what changes have happened over time.	Ref 5.3.11	Does your organisation offer a version management with the ability to track changes for all contracts and SLA?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.i DORA: - Art. 25.9	YES	See response to Ref 5.3.2. URLs referenced in the contract (including the SLAs) have a "Previous Versions" section.

Subchapter 5.4 Insurance

The contracts between CSPs and FIs should have an insurance clause that needs to increase with the number of assets on the cloud.	Ref 5.4.1	Does your organisation provide an insurance against risks for cloud usage?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.k	YES	Google will maintain insurance cover against a number of identified risks. In addition, Risk Manager gives you tools to leverage cyber insurance to deal with risks in the Google Cloud environment. https://cloud.google.com/risk-protection-program Google Cloud Financial Services Contract ref: Insurance
	Ref 5.4.2	Does your organisation provide, if applicable, the level of insurance cover requested?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 75.k	YES	Upon request, Google provides customers with certificates of insurance evidencing the insurance coverage. Google Cloud Financial Services Contract ref: Insurance
	Ref 5.4.3	Has your organisation regulated all the above requirements in the standard contract or a specific contractual amendment?		YES	This addressed in Google Cloud Financial Services Contract Google Cloud Financial Services Contract ref: Insurance

Chapter 6 - Portability

ECUC SECTION				CLOUD SERVICE PROVIDER SECTION	
Excerpt from the Position Paper 2.1	Ref. ID	Questions related to reg. reference / recognised standard (examples)	Reg. reference / recog. stand. (examples)	Offered / fulfilled by CSPs	Cloud Service Provider comment: If necessary, even to get a better understanding, please explain.
Subchapter 6.1 CSP should apply Technology Standards					
CSP should make sure to apply technology standards of internationally recognised institutes to their services. These include: - NIST (National Institute of Standards and Technology) - ISO (International Organization for Standardization) - CNCF (Cloud Native Computing Foundation) - an institute that implements the general requirements for the EU Cybersecurity Act (EUCA) e.g. BSI (Bundesamt für Sicherheit in der Informationstechnik): C5 (Cloud Computing Compliance Criteria Catalogue) - CSA (Cloud Security Alliance): STAR (Security, Trust, Assurance, and Risk) In order to prove the certification of the standards of these bodies, the adherence to these standards should be publicly documented by the CSP.	Ref 6.1.1	Does your organisation in general apply technology standards of international institutes to ensure interoperability and compatibility?	EBA/GL/2019/04 (ICT) Regulation (EU) 1025/2012: - ANNEX II Para 3, 4	YES	Google has attested to a number of international standards pertaining to interoperability and compatibility including, CSA STAR V4, NIST Publications (800-53, 800-171, 800-34), and ISO Standards (27701, 27110, 22301, 27018, 27017, 27001, 9001). In addition, Google Cloud has declared adherence to the SWIPO Data Portability Codes and has published our Transparency Statement which includes a mapping for Google Cloud. (https://cloud.google.com/security/compliance/swipo-codes; https://services.google.com/fh/files/misc/042022_swipo_transparency_statement.pdf)
	Ref 6.1.2	Does your organisation apply NIST to ensure interoperability and compatibility?	EBA/GL/2019/04 (ICT) Regulation (EU) 1025/2012: - ANNEX II Para 3, 4	YES	See response to Ref 6.1.1
	Ref 6.1.3	Does your organisation apply ISO to ensure interoperability and compatibility?	EBA/GL/2019/04 (ICT) Regulation (EU) 1025/2012: - ANNEX II Para 3, 4	YES	See response to Ref 6.1.1
	Ref 6.1.4	Does your organisation apply CNCF to ensure interoperability and compatibility?	EBA/GL/2019/04 (ICT) Regulation (EU) 1025/2012: - ANNEX II Para 3, 4	YES	Google Cloud is a contributor to CNCF Open Source projects, participating in CNCF training and certification programs helping to increase Kubernetes' reach. (https://cloud.google.com/blog/products/containers-kubernetes/google-cloud-credits-support-cncf-work-on-kubernetes; https://cloud.google.com/open-cloud)
	Ref 6.1.5	Does your organisation apply CSA to ensure interoperability and compatibility?	EBA/GL/2019/04 (ICT) Regulation (EU) 1025/2012: - ANNEX II Para 3, 4	YES	See response to Ref 6.1.1
	Ref 6.1.6	Does your organisation apply standards of other institutes which leverage interoperability and compatibility? Please specify in comment field which one.	EBA/GL/2019/04 (ICT) Regulation (EU) 1025/2012: - ANNEX II Para 3, 4	YES	See response to Ref 6.1.1
	Ref 6.1.7	Does your organisation publicly document the compliance with the confirmed standards to ensure interoperability and compatibility?	EBA/GL/2019/04 (ICT) Regulation (EU) 1025/2012: - ANNEX II Para 3, 4	YES	Google publicly documents our compliance with standards via our Compliance Offerings page and our Compliance Reports Manager. Compliance Offerings - https://cloud.google.com/security/compliance/offerings Compliance Reports Manager - https://cloud.google.com/security/compliance/compliance-reports-manager
Subchapter 6.2 CSP should offer Open-Source Technology and Standards					
CSP should embrace open-source technology and provide such components as software stacks, interfaces, and APIs. The provided services should build upon or be efficiently referable to open-source solutions from the open-source community. Effective pre-checks as part of the system lifecycle management should be in place before using open-source technology. This especially holds for standards in software, data, communication, and processes, which should be preferred in comparison to proprietary solutions.	Ref 6.2.1.	Does your organisation provide opensource technology in general as part of your product strategy to support the transfer of outsourced services to alternative providers ? Please specify your organisation´s strategy for open source and list in extracts the components being offered in the comment field.	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	Google is committed to the open source and open data communities. This commitment is manifested in our product strategy and services. (https://cloud.google.com/blog/topics/inside-google-cloud/empowering-customers-and-the-ecosystem-with-an-open-cloud ; https://cloud.google.com/open-cloud) Google has established a record of sharing technology through open source—from projects like Kubernetes, which is now the industry standard in container portability and interoperability in the cloud, to TensorFlow and Anthos, our hybrid and multi-cloud platform built on open technologies like Kubernetes, Istio, and Knative.

Subchapter 6.3 CSP should provide methods and tools to allow Workload Portability

CSPs should strongly support FIs to perform their exit plans for their workloads, services and applications as required by European Banking Authority (EBA) guidelines on outsourcing arrangements. CSPs should provide methods and tools to help migrate IaaS and PaaS to other IT service providers quickly and securely: - The methods and tools provided should enable a seamless migration to the most widely used commercial and open-source infrastructures, networks, platforms, and databases (state of the art technologies). Tools provided should enable homogeneous and heterogeneous migrations from any supported source within the CSP environment to a state-of-the-art technology target environment. - CSPs should provide tools to create infrastructure as a code-artifacts that describe existing resources and their properties in order to prepare for automated implementation in target environments. - Licenses for on-premises (or equivalent) solutions for a fair price to ensure clients have the option to return to an on-premises solution should an exit scenario occur. - For SaaS, the CSPs should offer a version/installation which is compatible with other cloud platforms or provides other alternatives, such as licenses for desktop installations. The exception here would be SaaS CSP proprietary solutions that needs cloud-native capabilities to provide the service(s) to the customer. Alternatives are especially relevant for Office products and should ensure that a migration during an exit is realistic and economically possible. CSPs should respect the requirement for FIs to have an exit plan.	Ref 6.3.1	Does your organisation supply methods and tools that enable customers a seamless migration to the most widely used commercial and open-source infrastructures, networks, platforms, and databases (state of the art technologies) to support the transfer of outsourced services to alternative providers?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	Data transfers from Google Cloud to alternate providers are supported on the Service API level, and in some cases, by data transfer services. (https://cloud.google.com/products/data-transfer) Supported media and file formats may depend on the infrastructure features used. Product specific documentation for exporting data from Google Cloud can be accessed here: https://cloud.google.com/docs/
	Ref 6.3.2	Does your organisation supply tools to create infrastructure as code-artifacts that describe existing resources and their properties in order to prepare for automated implementation in target environments to support the transfer of outsourced services to alternative providers?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	Google Cloud offers customers the use of APIs which enable them to export data from Google Cloud Platform. The types of artifacts that can be exported will vary by service. For example, typically container services support a larger scope of artifacts available for transfer. Customers can verify the artifacts available for transfer in the relevant service documentation: (https://cloud.google.com/docs) Google Cloud offers customers the ability to manage selected container artifacts. For example, code and build artifacts can be exported using the artifact registry: (https://cloud.google.com/artifact-registry) For Google Cloud Platform native artifacts, Google Cloud offers backup and restore, and Data export capabilities. Google has developed an open source tool, Terraformer, which enables customers to build Infrastructure as a code artificats from an existing infrastructure. - (https://github.com/GoogleCloudPlatform/terraformer) - (https://cloud.google.com/docs/terraform/resource-management/export?hl=en) Additionally, it is recommended that customers adopt open standards such as kubernetes and standard SQL connections to databases, using Google Cloud's managed service implementation of these standards. (https://cloud.google.com/kubernetes-engine) Google Cloud supports industry best practices in formats for exporting Data. Customers are free to export their Data from Google Cloud Platform for testing purposes. As Google Cloud Platform infrastructure and products are built to offer a wide range of capabilities, we recommend customers seek more detailed information about the formats for exporting data via service specific documentation: (https://cloud.google.com/products) Testing exported Data is dependent on the intended destination system. Therefore, it is recommended that once the planned destination system is known, Data export is tested against that system migration tool. For customers migrating to Google Cloud, we recommend that customers use the data migration guidance and Google Cloud trusted partners listed in the data migration pages (https://cloud.google.com/solutions/migration-center)
	Ref 6.3.3	Does your organisation support clients in returning existing licenses to an alternative solution if an exit scenario should occur to support the transfer of outsourced services to a different infrastructure?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	NO	Not applicable as Google Cloud is not a SaaS service.
	Ref 6.3.4	Does your organisation offer a version/installation which is compatible with other cloud platforms or provides other alternatives for the transfer of your SaaS offerings to alternative providers?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	NO	Not applicable as Google Cloud is not a SaaS service.
	Ref 6.3.5	Does your organisation have APIs or connectors for migration to other cloud platforms or provide alternatives?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	Data transfers from Google Cloud to alternate providers are supported on the Service API level, and in some cases, by data transfer services. (https://cloud.google.com/products/data-transfer) Supported media and file formats may depend on the infrastructure features used. Product specific documentation for exporting data from Google Cloud can be accessed here: (https://cloud.google.com/docs/.)

Subchapter 6.4 CSP should provide standardised Data Formats and Export Processes

CSP should provide standardised data formats and processes for data extraction and transport to other environments and platforms. The paragraph will only cover data portability and export requirements not already covered in other chapters, e.g. chapter 2 Requirements on Privacy: - CSP should establish bi-directional data portability by providing contract/service contract/SLA, processes, products, data formats, metadata and professional services to customers for all data owned as intellectual property by the customer.	Ref 6.4.1	To support the transfer of outsourced services to alternative providers, is data portability (information transfer, being export and import of data to and from other CSP) part of the standard contract?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	Google's Cloud Data Processing Addendum describes our commitment to data portability. (https://cloud.google.com/terms/data-processing-addendum)
	Ref 6.4.2	To facilitate the transfer of oursourced services and related data, is data portability part of the standard offered SLA?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para 107, 108	YES	See response to Ref 6.3.1 and Ref 6.3.2. Customers can choose to use a number of Google services/features to transfer their data. SLAs for Google services are listed here: https://cloud.google.com/terms/sla
	Ref 6.4.3	To facilitate the transfer of oursourced services and related data, is data portability supported by internal processes of your organisation?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	See response to Ref 6.3.1 and Ref 6.3.2. Google has established internal processes to ensure portability and interoperability, along with providing tools for exporting customer data in machine-readable formats where feasible.
	Ref 6.4.4	To facilitate the transfer of oursourced services and related data, is data portability supported by an information transfer registry?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	Google offers a number of Google Cloud product features including Resource Locations which allows customers to identify where resources are deployed and maintained by the services in use.
	Ref 6.4.5	To facilitate the transfer of oursourced services and related data, is data portability supported via different (common) data formats (e.g; JSON, XML)?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	This is service dependent. For example, customers can use the Migrate to Virtual Machines import and export feature to create, export, and/or revise migrating VMs using a CSV file. Customers should consult relevant product documentation. https://cloud.google.com/products
	Ref 6.4.6	To facilitate the transfer of outsourced services and related data, is data portability supported by means of appropriate physical data transfer media for different data volumes (small to very large)?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	Data transfers to Google Cloud are supported by Transfer Appliance services that support physical device transfers. Different types of data transfer: https://cloud.google.com/architecture/migration-to-google-cloud-transferring-your-large-datasets Physical data transfer media: https://cloud.google.com/transfer-appliance/docs/4.0/overview

	Ref 6.4.7	To facilitate the transfer of outsourced services and related data, is the exported data accompanied by its relevant meta-data and is this part of the above mentioned data formats?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	See response to Ref 6.4.6. Exported data is accompanied by relevant metadata.
	Ref 6.4.8	To facilitate the transfer of outsourced services and related data, are professional services offered to support the customer in his data portability process and implementation?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	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.
- Data portability includes both data and meta-data which give the data its meaning. Amongst others these are operational data, secrets, metadata and their backups as well.	Ref 6.4.9	To support the transfer of outsourced services and data to alternative providers is the provided data export containing operational meta-data (e.g. creation date & time)?	ISO/IEC 27018:2019: - Control 18.1 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	PARTIAL	This is service dependent. Customers should consult relevant product documentation. https://cloud.google.com/products
	Ref 6.4.10	To support the transfer of outsourced services and data to alternative providers, is the provided data export containing (in the same or separate export file) the secrets to decrypt the data?	GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	If data is ecnrypted using cloud native encryption, files are first decrypted and then exported. If the key is managed by the customer (either in Google Cloud, or externally), it is not possibile for Google to decrypt, or export the keys. For more information, customers can view the links below: - https://cloud.google.com/security-key-management - https://cloud.google.com/blog/products/identity-security/cloud-external-key-manager-now-in-beta
	Ref 6.4.11	To support the transfer of outsourced services and data to alternative providers, is the provided data export containing the meta-data of the meta-data itself (e.g. in order to understand if a date is a creation date or date of update)?	GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	PARTIAL	This is service dependent. Customers should consult relevant product documentation. (https://cloud.google.com/products)
	Ref 6.4.12	To support the transfer of outsourced services and data to alternative providers, is the provided data export containing a set of backup snap-shots?	GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	PARTIAL	This is service dependent. Customers should consult relevant product documentation. (https://cloud.google.com/products) For more information on creating and managing disk snapshots see here: (https://cloud.google.com/compute/docs/disks/create-snapshots)

Ref 6.4.13	To support the transfer of outsourced services and data from other providers to your organisation, can your organisation import a data file containing operational meta-data (e.g. creation date & time)?	GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	Google Cloud does import data files containing operational metadata. This metadata can be used to monitor the performance of customers' applications and infrastructure, to troubleshoot problems, and to optimize their usage of Google Cloud services. The following are some examples of operational metadata that can be imported into Google Cloud: - Cloud Logging logs: These logs contain information about customers' applications requests, responses, and errors. - Cloud Monitoring metrics: These metrics measure the performance of customers' applications and infrastructure. - Cloud Profiler profiles: These profiles capture information about customers' application's execution, such as the time it takes to execute different parts of their code. Customers can import operational metadata into Google Cloud using the following methods: - The Google Cloud Console: Customers can import data files into the Google Cloud Console by uploading them to the Cloud Logging or Cloud Monitoring datasets. - The Google Cloud SDK: Customers can import data files into Google Cloud using the gcloud command-line tool. - The Google Cloud API: Customers can import data files into Google Cloud using the Google Cloud API. Once Customers have imported operational metadata into Google Cloud, they can use it to monitor the performance of their applications and infrastructure, to troubleshoot problems, and to optimize their usage of Google Cloud services.
Ref 6.4.14	To support the transfer of outsourced services and data from other providers to your organisation, can your organisation import a data file containing (in the same or separate export file) the secrets to decrypt the data?	GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	Customers may be using existing cryptographic keys that were created on their premises or in an external key management system. If customers migrate an application to Google Cloud or if they add cryptographic support to an existing Google Cloud application, they can import the relevant keys into Cloud KMS. - Customers can import into Cloud HSM keys or software keys in Cloud KMS. - Key material is wrapped for protection in transit. Customers can use the Google Cloud CLI to automatically wrap the key, or they can wrap the key manually. (https://cloud.google.com/kms/docs/wrapping-a-key) - Google Cloud has access to the wrapping key only within the scope of the import job. For Cloud HSM keys, the wrapping key never resides outside of Cloud HSM. https://cloud.google.com/kms/docs/key-import?hl=en
Ref 6.4.15	To support the transfer of outsourced services and data from other providers to your organisation, can your organisation import a data file containing the meta-data of the meta-data itself (e.g. in order to understand if a date is a creation date or date of update)?	GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	Yes, Google Cloud can import a data file containing the meta-data of the meta-data itself (e.g. in order to understand if a date is a creation date or date of update). This is possible through the use of the Google Cloud Data Fusion service. Data Fusion is a fully managed, cloud-native, enterprise data integration service that makes it easy to create and manage data pipelines. Data Fusion can import data from a variety of sources, including files, databases, and SaaS applications. Once the data is imported, Data Fusion can be used to transform and enrich the data, and to load it into a variety of target destinations, including Google Cloud BigQuery, Google Cloud Storage, and Google Cloud SQL. (https://cloud.google.com/data-fusion)

	Ref 6.4.16	To support the transfer of outsourced services and data from other providers to your organisation, can your organisation import a data file containing a set of backup snap-shots?	GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	Yes, Google Cloud can import a data file containing a set of backup snapshots. Google Cloud offers a number of services that can be used to import backup snapshots, including: - Google Cloud Storage: Google Cloud Storage can be used to store backup snapshots. Backup snapshots can be stored in either standard or nearline storage. Standard storage is more expensive, but it offers better performance. Nearline storage is less expensive, but it offers slower performance. - Google Cloud Transfer Service: Google Cloud Transfer Service can be used to transfer backup snapshots from other providers to Google Cloud. Google Cloud Transfer Service offers a number of features that make it a good choice for transferring backup snapshots, including: - Support for a variety of protocols, including HTTP, FTP, and SFTP - Support for a variety of transfer speeds - Support for a variety of transfer sizes Once backup snapshots are stored in Google Cloud, they can be used to restore data that has been lost or damaged. Google Cloud offers a number of services that can be used to restore data from backup snapshots, including: - Google Cloud Compute Engine: Google Cloud Compute Engine can be used to restore data from backup snapshots to running virtual machines. - Google Cloud App Engine: Google Cloud App Engine can be used to restore data from backup snapshots to running applications. - Google Cloud SQL: Google Cloud SQL can be used to restore data from backup snapshots to databases. - Google Cloud BigQuery: Google Cloud BigQuery can be used to restore data from backup snapshots to data warehouses.
- CSPs should establish processes that support the customer to execute data portability and export. - CSPs should offer products and services that support the customer to execute bi-directional (in and out) online and offline (bulk) data portability. Data at rest and in transit should be secured and privacy needs to be ensured. - Customers must be able to choose data portability products and services depending on the urgency, the data volume to exchange, different data querying (e.g. SQL) and representation (e.g. JSON) formats and cost.	Ref 6.4.17	To support the transfer of outsourced services and data, does your organisation have a service to support customers to execute the data import/export processes?	ISO/IEC 27018:2019: - Control 16.11 GDPR: - Art. 20 EU Data Act: - Art. 24, 26 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	Customers can export their data from Google Cloud services in a number of industry standard formats. For example: Google Kubernetes Engine is a managed, production-ready environment that allows portability across different clouds as well as on premises environments. (https://cloud.google.com/kubernetes-engine/) Migrate for Anthos allows customers to move and convert workloads directly into containers in Google Kubernetes Engine. (https://cloud.google.com/migrate/containers) Customers can also export/import an entire VM image in the form of a .tar archive. Find more information on images and on storage options and the links here: https://cloud.google.com/compute/docs/images; https://cloud.google.com/compute/docs/disks/
	Ref 6.4.18	To support the transfer of outsourced services and data, is data portability supported by means of appropriate physical data transfer media for different data volumes (small to very large)?	ISO/IEC 27018:2019: - Control 13.2 GDPR: - Art. 20 EU Data Act: - Art. 29 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	See response to Ref 6.4.6
	Ref 6.4.19	Does your organisation provide an secure transfer of outsourced services and data? Please specify how the physical data transfer media ist protected at rest and in transit.	ISO/IEC 27018:2019: - Control 13.2 GDPR: - Art. 20 EU Data Act: - Art. 29 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	Data is encrypted on Transfer Appliance with dm-encrypt and partition-level encryption, with the AES-256 encryption algorithm. For more information: https://cloud.google.com/transfer-appliance/docs/4.0/security-and-encryption?hl=en

-CSPs should enable open market standards (cf. "The Open Data Institute") (additional requirements in paragraph on "Technology Standards") for: - Shared vocabulary (meta-data): Words, Models, Taxonomies & Identifiers - Data exchange: File formats, Schemas, Data types & Data transfer methods - Guidance: Codes of practice, how to collect data & Units and measures	Ref 6.4.20	To support the transfer of outsourced services and data, is data portability supported via different data formats (e.g; JSON, XML)?	GDPR: - Art. 20 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	Yes, Google Cloud supports data portability via different data formats (e.g. JSON, XML). Google Cloud offers a number of services that can be used to export data from Google Cloud in different data formats, including: - Google Cloud Storage: Google Cloud Storage can be used to export data from Google Cloud in JSON or XML format. - Google Cloud Dataproc: Google Cloud Dataproc can be used to export data from Google Cloud in JSON or XML format. - Google Cloud Data Fusion: Google Cloud Data Fusion can be used to export data from Google Cloud in JSON or XML format. Once data has been exported from Google Cloud in a specific data format, it can be imported into other locations in that same data format.
	Ref 6.4.21	To support the transfer of outsourced services and data, is data portability supported via different technical means: API based, file exchange (online and offline)?	GDPR: - Art. 20 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	Google offers both network transfer, and in case of large amounts of data, physical medium. More information: Cloud data transfer options: https://cloud.google.com/architecture/migration-to-google-cloud-transferring-your-large-datasets Cloud migration partners: https://cloud.google.com/solutions/cloud-migration-program
	Ref 6.4.22	To facilitate the transfer of outsourced services and data, is data portability supported with guidance codes of practice to support the customer in his data portability journey?	GDPR: - Art. 20 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107	YES	For customers migrating to Google Cloud, we recommend that customers use the data migration guidance and Google Cloud trusted partners listed in the data migration pages (https://cloud.google.com/solutions/migration-center)
Example open standards to comply with: - Egeria: opensource metadata standard, maintained by the LF AI & Data Foundation	Ref 6.4.23	To facilitate the transfer of outsourced services and data with open technical standards, is your organisation supporting integration with open standard adoption?	BCBS 239: - Principle 2 Art. 33 BSI: - Clause 21, 52 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4 EU Data Act: - Art. 29	YES	See response to Ref 6.2.1

Ref 6.4.24	Is your organisation adhering to any standard/Code of Conduct to facilitate the transfer of outsourced services and data with open technical standards?	BCBS 239: - Principle 2 Art. 33 BSI: - Clause 21, 52 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4 EU Data Act: - Art. 29	YES	Google Cloud adheres to a number of standards and codes of conduct to facilitate the transfer of outsourced services and data with open technical standards. These include: - OpenAPI: Google Cloud supports the OpenAPI standard, which is a standard way of describing APIs. This makes it easy for users to understand how to use Google Cloud APIs and to integrate them with their own applications. - RESTful: Google Cloud APIs are RESTful APIs. This means that they follow the REST architectural style, which is a set of guidelines for designing APIs that are easy to use and maintain. - OAuth 2.0: Google Cloud supports the OAuth 2.0 standard, which is a standard way of granting access to data. This makes it easy for users to grant access to Google Cloud data to their own applications without having to share their passwords. - OpenID Connect: Google Cloud supports the OpenID Connect standard, which is a standard way of authenticating users. This makes it easy for users to authenticate to Google Cloud services using their existing OpenID Connect credentials. Google has also attested to a number of international standards pertaining to interoperability and compatibility including, CSA STAR V4, NIST Publications (800-53, 800-171, 800-34), and ISO Standards (27701, 27110, 22301, 27018, 27017, 27001, 9001). In addition, Google Cloud has declared adherence to the SWIPO Data Portability Codes and has published our Transparency Statement which includes a mapping for Google Cloud. (https://cloud.google.com/security/compliance/swipo-codes; https://services.google.com/fh/files/misc/042022_swipo_transparency_statement.pdf)
Ref 6.4.25	Is your organisation adhering to any standard/IaaS Code of Conduct Transparency Statement to facilitate the transfer of outsourced services and data with open technical standards?	BCBS 239: - Principle 2 Art. 33 BSI: - Clause 21, 52 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4 EU Data Act: - Art. 29	YES	See response to Ref 6.1.1
Ref 6.4.26	Is your organisation adhering to any standard/SaaS Code of Conduct to facilitate the transfer of outsourced services and data with open technical standards?	BCBS 239: - Principle 2 Art. 33 BSI: - Clause 21, 52 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4 EU Data Act: - Art. 29	NO	Not applicable as Google Cloud is not a SaaS service.
Ref 6.4.27	Is your organisation able to provide any Adherence Declaration Form to facilitate the transfer of outsourced services and data with open technical standards ?	BCBS 239: Principle 2 Art. 33 BSI: - Clause 21, 52 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4 EU Data Act: - Art. 29	YES	See response to Ref 6.1.1

- Where requested by the customer, the CSP should offer professional services in support of data portability and export.	Ref 6.4.28	To facilitate the transfer of outsourced services and data with open technical standards, are professional services offered to support the customer in his data portability process and implementation? (overlap with Q6.4.3-1)	BCBS 239: - Principle 2 Art. 33 BSI: - Clause 21, 52 GDPR: - Art. 30 Regulation (EU) 1025/2012: - ANNEX II Para 3, 4 EU Data Act: - Art. 29	YES	See response to Ref 6.4.8

Subchapter 6.5 CSP should be transparent with Ingress and Egress Costs

CSPs charge customers when they export data (so called egress cost) from the cloud to anywhere else. Compared to importing data exporting data is usually more expensive. Portability of applications and data is required in certain scenarios and in most cases part of the required exit strategy. FIs must have an exit strategy in place. The cost of leaving a cloud infrastructure or a service due to substantial egress cost is in contrast to this requirement: CSPs should provide ways for temporary and agreed exceptions to the costs and be transparent about the pricing. That in case an exit is required it can be achieved in an economical way.	Ref 6.5.1	Does your organisation document ingress and egress costs at a comparable level for the respective services to asses the financial resources of exits plan?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107, 108	YES	Google does not charge fees specifically related to data importing or related procedures. Standard storage and processing fees do apply and are provided to the customer. Example of fees charged for cloud storage: (https://cloud.google.com/storage/pricing)
	Ref 6.5.2	Does your organisation provide ways or plans that egress costs can be temporary lower or fixed to maintain the feasibility of exit plans?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107, 108	PARTIAL	Google Cloud's pricing remains transparent and innovative, including a number of ways to plan for egress costs: - Monitor egress costs: Customers can use the Google Cloud Console to monitor their egress costs. The Console shows customers how much data they have egressed from Google Cloud over a period of time. Customers can use this information to identify ways to reduce their egress costs. Customers can also view Google's network service tiers pricing page for more information on egress pricing. - https://cloud.google.com/network-tiers/pricing - https://cloud.google.com/vpc/network-pricing#internet_egress - https://cloud.google.com/storage/pricing#network-pricing - Use a load balancer: A load balancer can help customers to distribute traffic across multiple Google Cloud regions. This can help customers to reduce their egress costs by reducing the amount of data that needs to be egressed from any one region. - Estimate costs: Customers can gain an understanding of how theirr costs can fluctuate based on location, workloads, and other variables with the Google Cloud Pricing Calculator. https://cloud.google.com/products/calculator For a list of cost management tools, see here: https://cloud.google.com/cost-management
	Ref 6.5.3	Does your organisation specify and document ingress and egress on a contract level to support business plans and to maintain the feasibility of exit plans?	EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107, 108	YES	Prices and fee information are also publicly available on our SKUs page. Refer to our Pricing page for more information.

Subchapter 6.6 CSP should provide detailed Information on Data Center Location

FIs should know CSPs' data center physical locations to ensure proper planning for resilience and portability. Data Center information within every availability zone or region needs to be provided in a standardised format and made available directly to FIs as part of contractual obligations. Information is needed to support: - Mitigation of risks of CSP data center outages and impacts of regional disaster events impacting multiple CSP data centers - A clear understanding that each data center has access to separate power supplies and utility services as well as redundant paths that are isolated from the other data centers (in the same location / region).	Ref 6.6.1	Does your organisation provide information within zones and regions upon assigned data centers and their respective locations?	EBA/GL/2019/04 (ICT): - 3.2.3. Art. 8	YES	The locations of Google data centers are described at: - https://cloud.google.com/about/locations/
	Ref 6.6.2	Does your organisation in principle add this information to the contracts and service level agreements with FIs?	EBA/GL/2019/04 (ICT): - 3.2.3. Art. 8	YES	See the Data Center Information section in our Cloud Data Processing Addendum: https://cloud.google.com/terms/data-processing-addendum
	Ref 6.6.3	Does your organisation document and make available the seperation criteria of regions/zones/data centers to ensure the effectiveness of the risk-mitigating measures of exit plans?	EBA/GL/2019/04 (ICT): - 3.2.3. Art. 8	YES	Google operates multi-zone data centers all over the world, providing resilience in the event of localised or even region-wide environmental or infrastructure events. Information about the location of Google's facilities and where individual GCP services can be deployed is available on our Global Locations page.

Subchapter 6.7 CSP should safeguard Interoperability of selected Data Centers

It is common to establish at least two interoperable but independent data center locations, meeting national localisation requirements for redundant implementation to shift workload and to allow disaster recovery. Examples of standards to be implemented in the CSP Data Center migration solution: - Service modelling: Open-SCA (Software Composition and Analysis), USDL/SoaML/CloudML (multi-view services), EMML (mashups) - Service interfaces: OCCI (infrastructure management), CIMI (infrastructure management), EC2 (de-facto standard), TOSCA (portability), CDMI (data management) - Infrastructure: OVF (Open Virtualization Format for software on virtual machines) - CSPs should provide a managed and supported data center migration option leveraging existing standards according to the related domains.	Ref 6.7.1	Does your organisation provide supporting modules like SCA, USDL/SoaML/CloudML, EMML or equivalent solutions to facilitate undue disruption of business activities? Please specify in the comment field.	IEEE 2302-2021 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107, 108	YES	All of Google's data centers run on in independent but interopeable manner, relying on redunadant infrastructure and interopreable standards to ensure reliability. In operating multi-zone data centers in a geographically distributed environment, Google safeguards interoperability through a distributed system that is able to store and transfer data across many servers in separate data centers. In addition, In addition, Google Cloud has declared adherence to the SWIPO Data Portability Codes and has published our Transparency Statement which includes a mapping for Google Cloud. (https://cloud.google.com/security/compliance/swipo-codes; https://services.google.com/fh/files/misc/042022_swipo_transparency_statement.pdf)
	Ref 6.7.2	Does your organisation provide OCCI, CIMI, EC2, TOSCA, CDMI or equivalent solutions to facilitate undue disruption of business activities? Please specify in the comment field.	IEEE 2302-2021 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107, 108	YES	Google provides a suite of management tools for managing cloud services and resources on an ongoing basis: - **Cloud Console** is a web-based graphical user interface that customers can use to manage their GCP resources. (https://cloud.google.com/cloud-console) - **Google Cloud Operations** is an integrated monitoring, logging, and diagnostics hosted solution that helps customers gain insight into their applications that run on GCP, including availability and uptime of the services. (https://cloud.google.com/monitoring/) - **Resource Manager** allows customers to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow customers to group and hierarchically organize other Google Cloud Platform resources. (https://cloud.google.com/resource-manager/) - **Cloud Deployment Manager** is a hosted configuration tool that allows developers and administrators to provision and manage their infrastructure on Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources. (https://cloud.google.com/deployment-manager) - **Terraform on Google Cloud** is an open source tool that lets customers provision Google Cloud resources with declarative configuration files. (https://cloud.google.com/docs/terraform) - **Anthos Config Management** enables customers to automatically deploy shared environment configurations and services like Cloud Storage through Config Connector integration. (https://cloud.google.com/anthos/config-management)
	Ref 6.7.3	Does your organisation provide OVF for software packaging and distribution, or equivalent solutions to facilitate undue disruption of business activities? Please specify in the comment field.	IEEE 2302-2021 EBA/GL/2019/02 (Outsourcing): - Chap. 4 Para. 107, 108	YES	Customers can import VMs that are in OVF format to Compute Engine, whether they are in an OVF package or in an OVA single file. In addition, Google supports several virtual disk file formats, including VMDK, VHD and RAW.
Subchapter 6.8 CSP should run independent Network Connections					
CSPs should establish and provide multiple independent network connection options to ensure that communication and applications, are still available in the chosen data centers/regions when (hazardous) incidents occur. Also, operational and scheduled maintenance of these network connection must be independent and respect clients' configuration, ensuring that no back-up connection is unintentionally stopped. In more detail, it should be ensured that at least one stable connection is provided by the CSP at all times and that backup and main connections are not in maintenance mode at the same time.	Ref 6.8.1	Does your organisation provide and establish multiple independent network connections for a proper ICT operations management? Please specify your approach or refer to public documentation in comment field.	EBA/GL/2019/04 (ICT): - 3.5 ff, 3.4.4. Art. 36 ISO/IEC 27001:2013	YES	Google does not rely on any one specific data center for its continued operation and allocates redundant equipment, applications, services and data across multiple data centers. Google's production services are designed with hardware redundancy, multi-homing and automatic failover. This is discussed in Google's security whitepaper: https://cloud.google.com/security/overview/whitepaper Google Engineering implements a redundant architecture built on redundant telecommunication backbones that are a requirement for use with all Google data centers. Redundant network paths are implemented for all active nodes within the Google infrastructure to eliminate points of failure. All alternative processing/storage sites are active data centers. Given this model, there is no time period for resuming telecommunications when the primary telecommunications capabilities are unavailable.
	Ref 6.8.2	Does your organisation operate and maintain (FI's) network connection indepent for a proper ICT operations management?	EBA/GL/2019/04 (ICT): - 3.5 ff, 3.4.4. Art. 36 ISO/IEC 27001:2013	YES	See response to Ref 6.8.1