Google Cloud Whitepaper
February 2020

Data residency, operational transparency, and privacy for European customers on Google Cloud

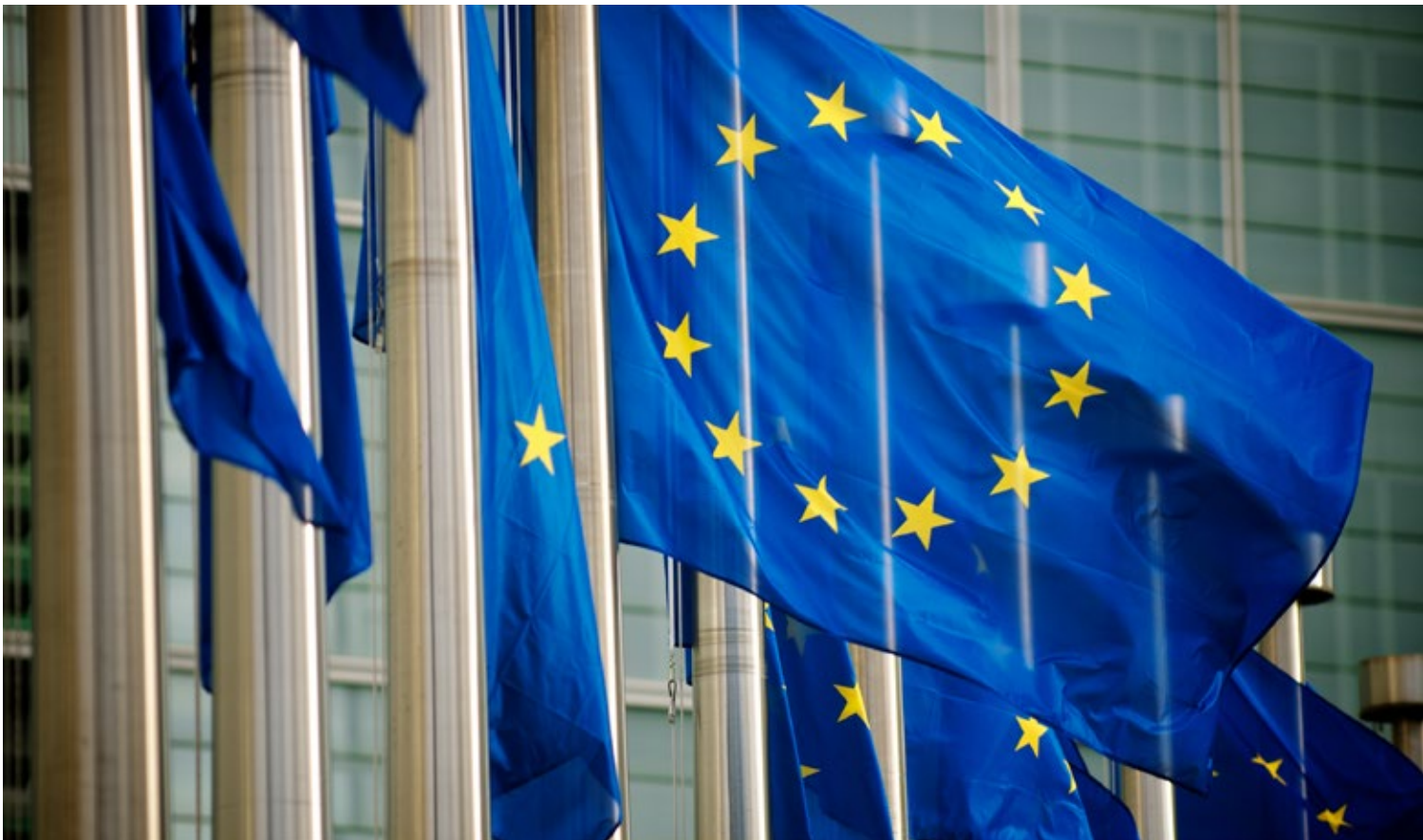
The information contained herein is intended to outline general product direction and should not be relied upon in making purchasing decisions nor shall it be used to trade in the securities of Alphabet Inc. The content is for informational purposes only and may not be incorporated into any contract. The information presented is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Any references to the development, release, and timing of any features or functionality described for these services remains at Google's sole discretion. Product capabilities, timeframes and features are subject to change and should not be viewed as Google commitments.

Google Cloud

Introduction

At Google Cloud, the privacy and security of customer data underpins the design of all of the services that we offer. We recognize that our global customers have specific concerns based on their regional and industry-specific requirements. While this whitepaper is directed towards our European customers, many of the topics addressed are not unique to Europe. This whitepaper describes options customers have for configuring services to meet their privacy and security requirements when using Google Cloud. Cloud users around the world have similar needs, and Google Cloud's Trust Principles[1] apply to all of our customers in every region. The content in this whitepaper is intended to be for informational purposes only, and is not legal advice. If you require it, you should seek independent legal advice relating to your status and obligations as a Google Cloud customer in Europe.

For our customers in Europe, common concerns may include compliance with the General Data Protection Regulation (GDPR), as well as sector-specific regulatory compliance requirements, such as the European Banking Authority (EBA) Guidelines. Customers may also have questions involving where their data is stored (data residency), how access to that data is controlled, and how we handle government requests and the CLOUD Act. We understand that data residency, operational transparency, and privacy on Google Cloud are top of mind for our European customers, and we are committed to offering the tools to meet these critical needs and preferences.



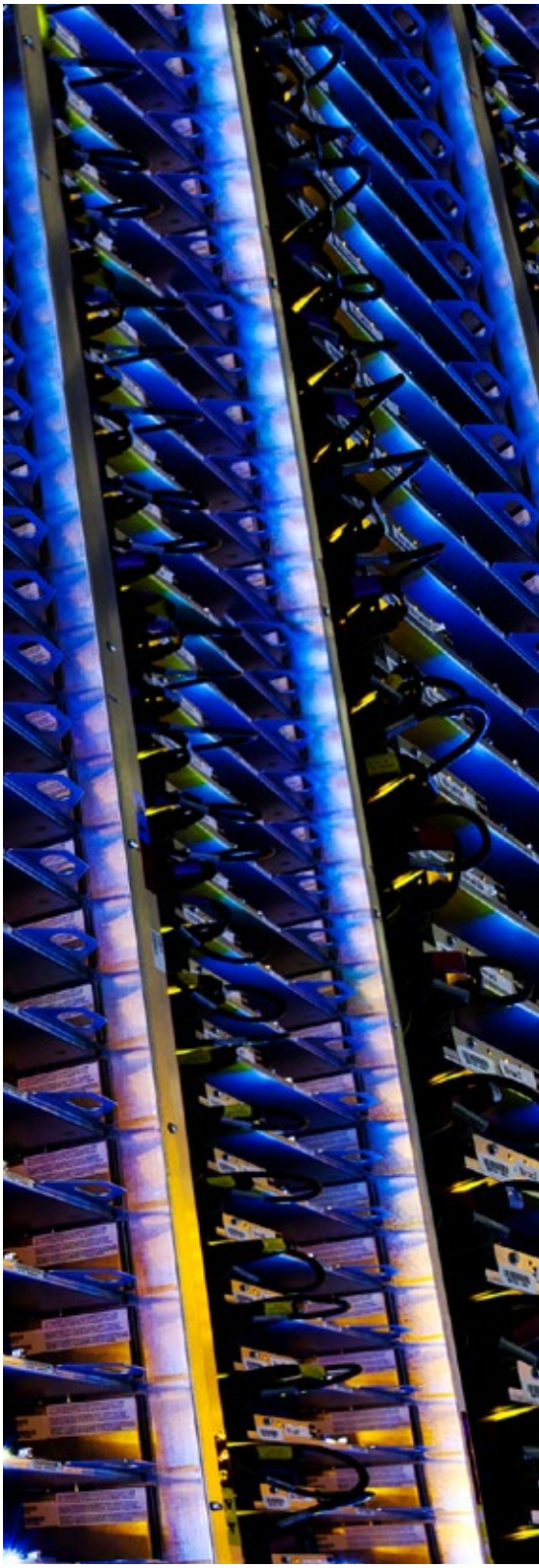
Data storage & data access

Google Cloud provides you with the ability to control where your data is stored. In Europe, our compute and storage key services[2] allow you to store customer data in regions[3] in the UK, Belgium, Germany, Finland, Switzerland, and the Netherlands, with a new planned region in Poland, and several others forthcoming.[4]

When you choose to configure resources in these locations for our compute and storage key services, Google will store that customer data at rest only in the selected region, in accordance with our Service Specific Terms[5] and Terms of Service.

To assist our customers in enforcing these controls, Google Cloud offers Organization Policy[6] constraints, which can be applied at the organization, folder, or project level. You can limit the physical location of a new resource with the Organization Policy Service resource locations constraint.[7] When coupled with Cloud IAM configuration,[8] which helps you to define fine-grained access policies and precisely control access to Google Cloud hosted data, you can prevent your employees from accidentally storing customer data in the wrong Google Cloud region.

Google Cloud also provides you with the ability to control the network locations from which users can access data by using VPC Service Controls.[9] This product allows you to limit access to users by IP address filtering, and Cloud Armor[10] allows restricting your external load balancer ingress to a specific region. You can even use this constraint if the user is authorized according to your Cloud IAM[11] policy. Using VPC Service Controls, you create a service perimeter[12] which defines the virtual boundaries from which a service can be accessed, preventing customer data from being moved outside of those boundaries. It also helps mitigate risks such as the misconfiguration of employee access controls or attackers taking advantage of compromised accounts. Identity-Aware Proxy (IAP)[13] enables customers to control access to cloud applications and VMs based on the user's identity and the context of their request. We also allow the creation of a perimeter that permits limited external access[14] if desired.

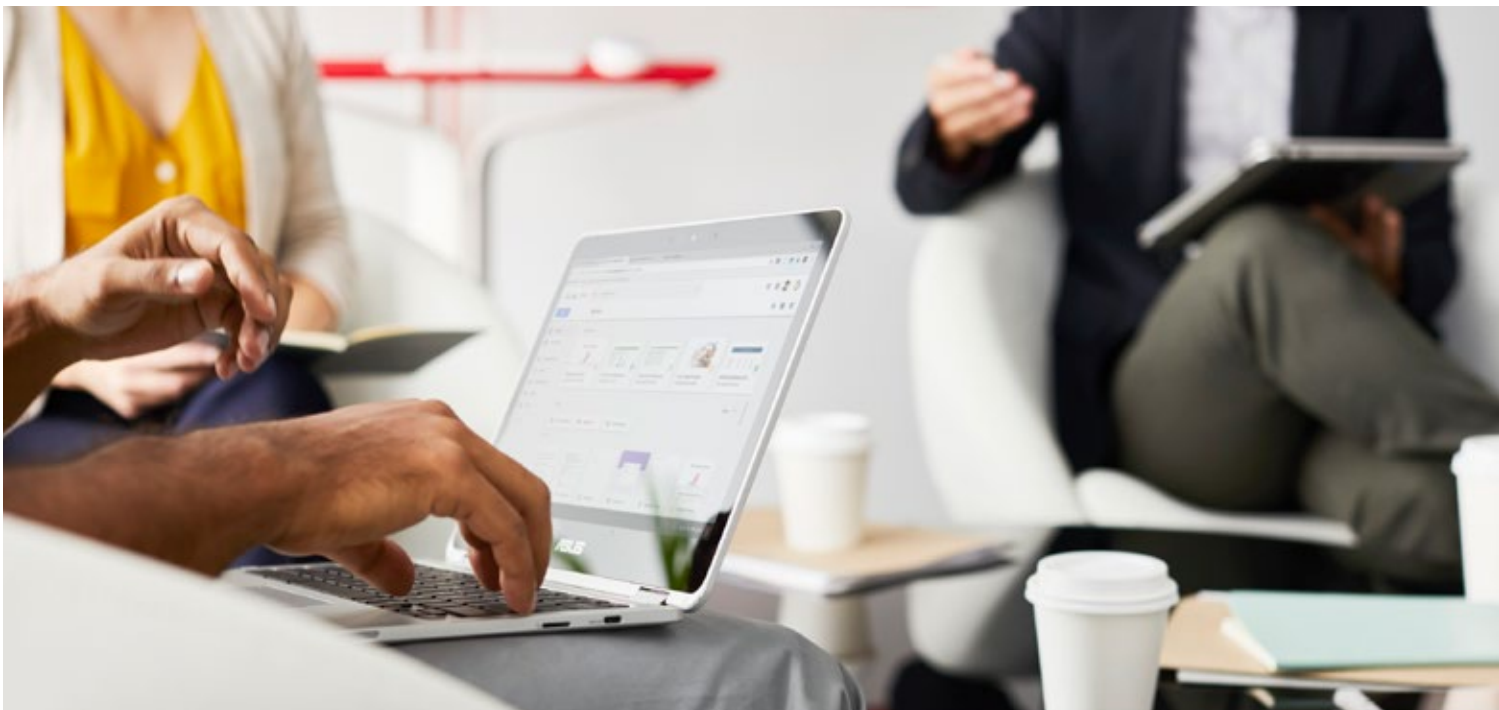


Encryption key management

For many operations, you may want to transfer your data between GCP's regions. Google Cloud enables encryption in transit[15] by default to encrypt inter-region traffic that is outside the perimeter of Google's facilities. Whenever data is stored, Google Cloud applies encryption at rest[16] by default. To gain more control over how data is encrypted at rest, Google Cloud customers can use our Cloud Key Management Service (Cloud KMS)[17] to generate, use, rotate, and destroy encryption keys according to the customers' own policies, a control we refer to as customer-managed encryption keys (CMEK). If you are using Cloud KMS,[18] your cryptographic keys must be stored in the region where you deploy the resource. You can also choose to store your keys in the region you choose with our Cloud Hardware Security Module (HSM)[19] service, which allows customers to host encryption keys and perform cryptographic operations in FIPS 140-2 Level 3 certified HSMs.

Customers can also implement Customer Supplied Encryption Keys (CSEK)[20] for supported services so that GCP encrypts data with customer-supplied keys and purges the supplied keys from memory after the customer requested operation is complete.

We also offer External Key Manager (Cloud EKM),[21] which allows you to store and manage keys in a third-party key management product deployed outside of Google's infrastructure. Using a third-party product allows you to place a KMS key ring in a geographic location of your choice or in one of the regions[22] recommended by your external key manager. You can use Cloud EKM in any specific (i.e. non-global) Google Cloud region supported for Cloud KMS.



Cloud administrator access

On GCP, you can configure Cloud IAM permissions[23] to limit access by your own administrators, curating the right amount of access at the project, folder or dataset level. This includes an extensive list of permissions and the predefined roles[24] that grant them. You can also create your own custom roles[25] that contain exactly the permissions you specify.

We also allow you to control access by Google personnel. Access Approval[26] allows you to require explicit approval before any personnel accesses your data or configurations on GCP, unless those accesses are necessary to resolve a current service disruption, security incident, or legal requirement.* This functionality is available to Platinum or Enterprise (Role-based) support customers on GCP. Access Approval works by sending customers an email and/or Cloud Pub/Sub message with an access request that the customer is able to approve. Using the information in the message, customers can use the GCP Console or the Access Approval API to approve the access.

Access Approval for GCP complements the visibility provided by Access Transparency,[27] which generates near real-time logs when Google administrators interact with your data, including the office location of the administrator and the reason for the access. Coming soon, you'll be able to enforce specific attributes for administrators who are allowed to access your data or configurations—including the geographic region from which they are operating and other compliance-relevant attributes.

Key Access Justifications,[28] an upcoming feature that works with Cloud KMS and External Key Manager, provides a detailed justification each time one of your keys is requested to decrypt data, along with a mechanism for you to approve or deny the key access, using an automated policy that you set. This product provides visibility into every request for an encryption key that permits data to change state from at-rest to in-use, with a justification for that request. It includes a commitment from GCP to protect the integrity of our controls and the justifications. Using Key Access Justifications with External Key Manager (initially with BigQuery and Google Compute Engine/Persistent Disk), you can deny Google the ability to decrypt your data for any reason.

* The comprehensive list of Access Approval exclusions can be found at https://cloud.google.com/access-approval/docs/overview

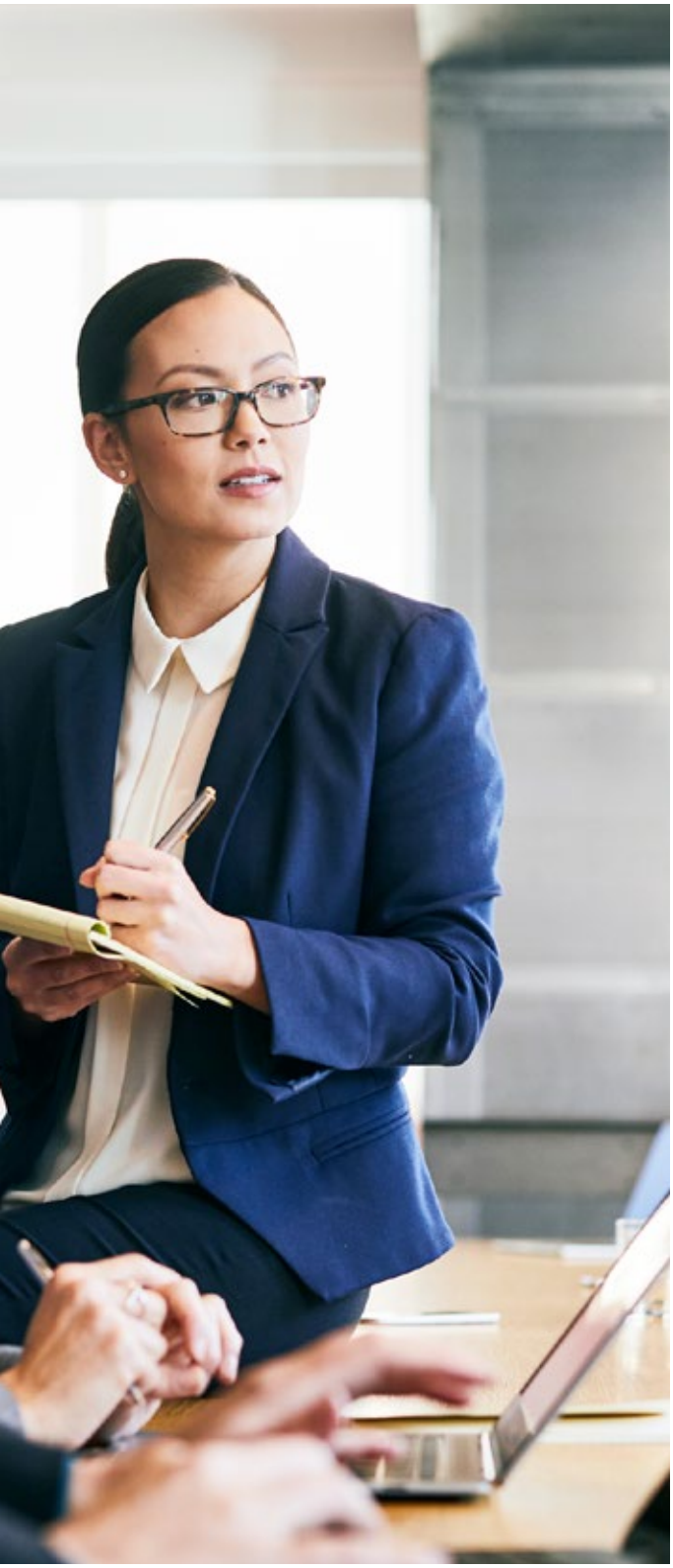
Government requests for customer data

One particular situation that is of interest to our customers and partners in Europe relates to requests for data from government agencies and, more recently, the impact of the U.S. CLOUD Act[29] and the U.S./U.K. Agreement[30] on the privacy and security of our customers' data.

The CLOUD Act and the recently announced U.S./U.K. Agreement[31] do not change how Google handles government requests to disclose enterprise customer data.[32] Our team reviews and evaluates each and every one of the requests we receive for legal validity and appropriate scope, as well as for compliance with international human rights standards, our own policies, and applicable law.

Generally speaking, if customer data is sought during the course of a legitimate legal investigation, Google informs the government that it should request customer data directly from the organization in question. This approach is in line with the U.S. Department of Justice's policy[33] that prosecutors should go to customers directly. It is also in line with EU policy proposals.[34]

However, if Google does receive a direct government data request regarding a customer account, we have a team of lawyers and trained personnel dedicated to reviewing requests. Each data request is reviewed using the following guidelines; note that we follow the same process for CLOUD Act data requests.



1. **Respect for the privacy and security of the data customers store with Google.** Each request is reviewed to make sure it satisfies international human rights standards, our own policies, and the law. If we believe a request is overly broad, we'll seek to narrow it. Google has opposed indefinite non-disclosure orders[35] and has fought for the right to notify customers of government requests for data. We do not provide "backdoor" direct access to any government and we do not hesitate to protect customer interests.

2. **Customer notification.** At a minimum, governments should provide direct notification to customers[36] when they seek to compel cloud service providers to disclose data. Except in emergency situations involving a threat to life, it is our policy to notify the customer before any information is disclosed unless such notification is prohibited by law. We will provide delayed notice to users after a legal prohibition is lifted, such as when a statutory or court ordered disclosure prohibition period has expired. This notification typically goes to the customer's point of contact.

3. **Consideration of customer objections.** 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.

   For U.S. government data requests, if Google notifies the customer of the 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.

Compliance controls and support

Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google Cloud undergoes several independent third-party audits on a regular basis to provide this assurance. Some of the key international and European standards we are audited against are:

- ISO/IEC 27001 (Information Security Management)[37]
- ISO/IEC 27017 (Cloud Security)[38]
- ISO/IEC 27018 (Cloud Privacy)[39]
- SOC 2[40] and SOC 3[41] reports
- C5 (German Federal Office for Information Security (BSI))[42]

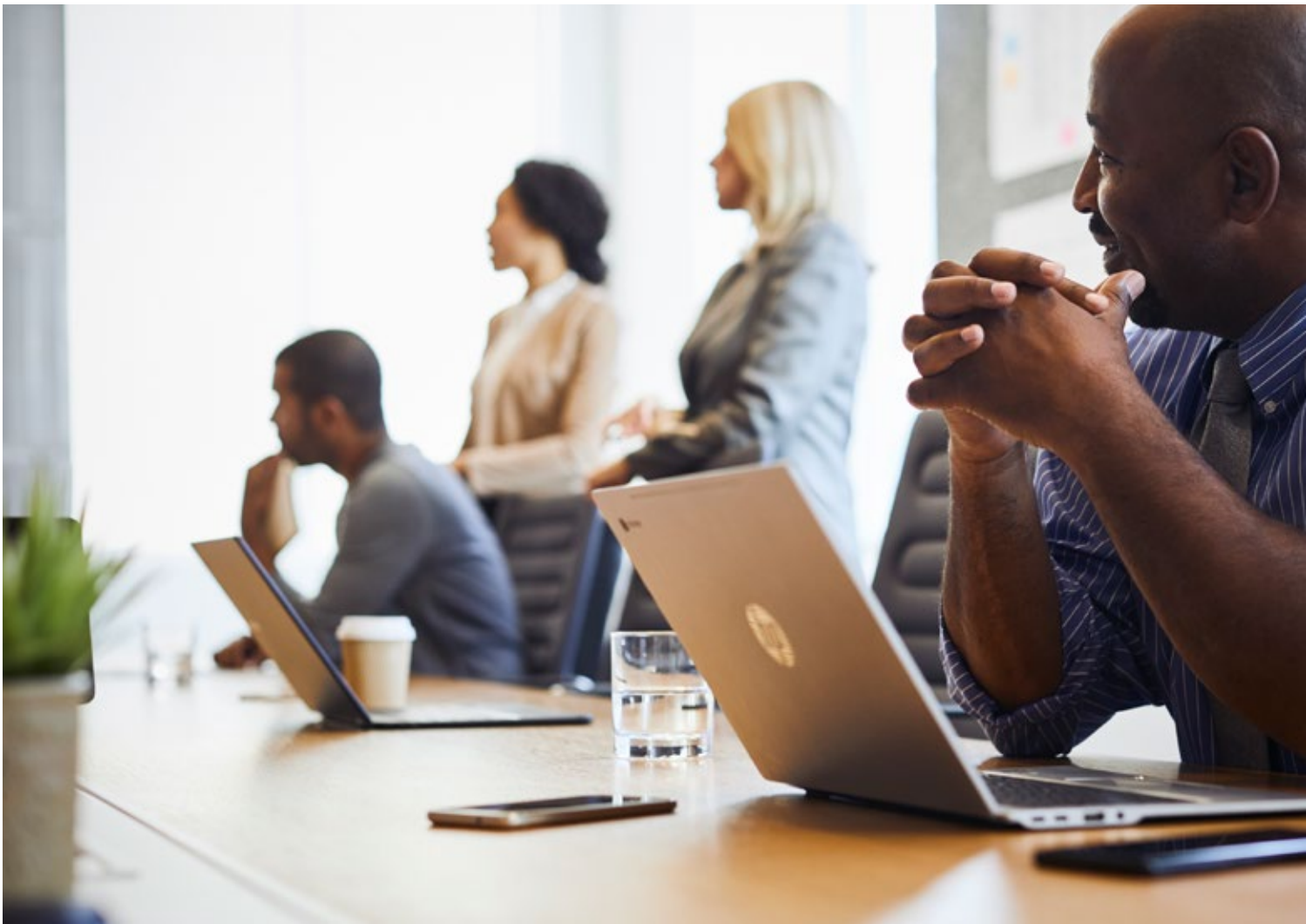
Google also participates in sector and country-specific frameworks. For example, for companies working in and with the French healthcare sector, it is important that Google Cloud is HDS-certified[43] Additionally, Google provides offerings such as the ISAE 3000 Type 2 Report,[44] which verifies the effectiveness of Google's internal controls to support adherence to certain FINMA (the Swiss Financial Market Supervisory Authority) requirements applicable to regulated financial services customers. Where formal certifications or attestations may not be required or applied, we also provide resource documents and mappings to frameworks and laws, such as the EBA Outsourcing Guidelines[45] and the GDPR.[46] A complete list of our compliance offerings is available via our Compliance resource center.[47]

We also understand that regulations such as GDPR place significant emphasis on enterprises knowing how their data is being processed, who has access to data, and how security incidents will be managed. It's important to note that GDPR compliance is a shared responsibility. Google Cloud generally acts as a data processor of customer data, and as a data processor we process that data only as instructed by you—our customers. In turn, you own your data, and Google Cloud is committed to providing you with tools and resources that put you in control of your data. Our data processing terms for G Suite[48] and Google Cloud Platform[49] are designed to directly address GDPR requirements. These contractual commitments clearly articulate our privacy commitments to customers, and are fundamental to GDPR compliance for both Google and our Cloud customers. We provide GDPR-related documentation, white papers, videos, and other useful information for customers on our GDPR Resource Center,[50] as well as our GDPR overview page.[51]

Conclusion

At Google Cloud, we work hard to earn and maintain your trust by giving you a clear and detailed understanding of our process and approach to security. The capabilities outlined in this whitepaper create a solution that gives you control over the location of your data and access to that data. With these considerations addressed, our customers in Europe and around the globe can confidently build mission critical workloads on Google Cloud. Even so, we're not done yet: we continue to invest in data privacy and security innovations to anticipate the future needs of our customers so that they can move to Google Cloud today knowing that they are fortified for the future.

To learn more about our capabilities, you can read our Trust whitepapers for GCP[52] and G Suite,[53] and visit our Trust & Security site.[54]



Appendix

Page 2:

[1] Google Cloud Trust Principles: https://cloud.google.com/security/privacy

Page 3:

[2] Google Cloud Platform Key Services: https://cloud.google.com/terms/key-services
[3,4] Google Cloud locations: https://cloud.google.com/about/locations
[5] Google Cloud Service Specific Terms: https://cloud.google.com/terms/service-terms
[6,7] Restricing Resource Locations: https://cloud.google.com/resource-manager/docs/organization-policy/defining-locations
[8] Cloud IAM configuration: https://cloud.google.com/service-usage/docs/reference/rest/v1/services/enable
[9] Overview of VPC Service Controls: https://cloud.google.com/vpc-service-controls/docs/overview
[10] Cloud Armor: https://cloud.google.com/armor
[11] Cloud Identity and Access Management: https://cloud.google.com/iam
[12] VPC Service Controls: Creating a service perimeter: https://cloud.google.com/vpc-service-controls/docs/create-service-perimeters
[13] Google Cloud Identity-Aware Proxy: https://cloud.google.com/iap
[14] VPC Service Controls: Enabling controlled access when creating a perimeter: https://cloud.google.com/vpc-service-controls/docs/create-service-perimeters#external-access

Page 4:

[15] Encryption in Transit in Google Cloud: https://cloud.google.com/security/encryption-in-transit
[16] Encryption at rest: https://cloud.google.com/security/encryption-at-rest
[17,18] Google Cloud Key Management Service: https://cloud.google.com/kms
[19] Google Cloud Hardware Security Module: https://cloud.google.com/hsm
[20] Customer-Supplied Encryption Keys: https://cloud.google.com/security/encryption-at-rest/customer-supplied-encryption-keys
[21] Google Cloud External Key Manager: https://cloud.google.com/ekm
[22] Google Cloud locations: https://cloud.google.com/about/locations

Page 5:

[23] Google Cloud IAM permissions reference: https://cloud.google.com/iam/docs/permissions-reference
[24] Cloud IAM: Understanding roles: https://cloud.google.com/iam/docs/understanding-roles
[25] Cloud IAM: Creating and managing custom roles: https://cloud.google.com/iam/docs/creating-custom-roles
[26] Access Approval documentation: https://cloud.google.com/access-approval/docs
[27] Access Transparency: https://cloud.google.com/access-transparency
[28] Key Access Justifications: https://cloud.google.com/blog/products/identity-security/control-access-to-gcp-data-with-key-access-justifications

Page 6:

[29] U.S. Cloud Act: https://www.justice.gov/dag/page/file/1152896/download
[30,31] U.S./U.K. Agreement: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf
[32] Goverment requests for customer data: controlling access to your data in Google Cloud whitepaper: https://services.google.com/fh/files/blogs/government_access_technical_whitepaper.pdf
[33] Seeking enterprise customer data held by cloud service providers: https://www.justice.gov/criminal-ccips/file/1017511/download
[34] EU policy proposal: https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF

Page 7:

[35] Advancing customer control in the cloud: https://cloud.google.com/blog/topics/inside-google-cloud/advancing-customer-control-in-the-cloud
[36] Written testimony of Richard Salgado: https://www.judiciary.senate.gov/imo/media/doc/09-16-15%20Salgado%20Testimony.pdf

Page 8:

37 Google Cloud Compliance Resource Center: ISO/IEC 27001: https://cloud.google.com/security/compliance/iso-27001
38 Google Cloud Compliance Resource Center: ISO/IEC 27017: https://cloud.google.com/security/compliance/iso-27017
39 Google Cloud Compliance Resource Center: ISO/IEC 27018: https://cloud.google.com/security/compliance/iso-27018
40 Google Cloud Compliance Resource Center: SOC 2: https://cloud.google.com/security/compliance/soc-2
41 Google Cloud Compliance Resource Center: SOC 3: https://cloud.google.com/security/compliance/soc-3
42 Google Cloud Compliance Resource Center: Cloud Computing Compliance Controls Catalogue (C5): https://cloud.google.com/security/compliance/bsi-c5
43 Google Cloud Compliance Resource Center: HDS: https://cloud.google.com/security/compliance/hds
44 Google Cloud Compliance Resource Center: ISAE 3000 Type 2 Report: https://cloud.google.com/security/compliance/isae-3000-type-2
45 Google Cloud Compliance Resource Center: EBA Outsourcing Guidelines: https://cloud.google.com/security/compliance/eba-outsourcing-guidelines
46,51 Google Cloud & the General Data Protection Regulation (GDPR): https://cloud.google.com/security/gdpr
47 Google Cloud Compliance Resource Center: https://cloud.google.com/security/compliance
48 Data Processing Amendment to G Suite and/or Complementary Product Agreement: https://gsuite.google.com/terms/dpa_terms.html
49 Google Cloud Data Processing and Security Terms: https://cloud.google.com/terms/data-processing-terms
50 GDPR Resource Center: https://cloud.google.com/security/gdpr/resource-center

Page 9:

52 Trusting your data with Google Cloud Platform whitepaper: https://cloud.google.com/files/gcp-trust-whitepaper.pdf
53 Trusting your data with G Suite whitepaper: https://cloud.google.com/files/gsuite-trust-whitepaper.pdf
54 Google Cloud Trust & security: https://cloud.google.com/security/