Per ulteriori risorse, fare riferimento al Centro risorse per la privacy (https://cloud.google.com/privacy?hl=it) di Google Cloud (https://cloud.google.com/privacy?hl=it)

Torna al Centro risorse sulla privacy (https://cloud.google.com/privacy/?hl=it)

Google Cloud e il Regolamento generale sulla protezione dei dati (GDPR)

Il Regolamento generale sulla protezione dei dati (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679) (GDPR) è una normativa sulla privacy che ha sostituito la Direttiva 95/46/CE sulla protezione (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN?utm_medium=et&utm_source=google.com%2Fcloud&utm_campaign=gdpr&utm_content=gdpr_faqs) dei dati del 24 ottobre 1995 del 25 maggio 2018. Il GDPR stabilisce requisiti specifici per le imprese e le organizzazioni con sede in Europa o che servire gli utenti in Europa. Esso:

- Regola il modo in cui le aziende possono raccogliere, utilizzare e archiviare i dati personali
- Si basa sulla documentazione attuale e sui requisiti di rendicontazione per aumentare la responsabilità
- Autorizza sanzioni alle impr

In Google Cloud, sosteniamo iniz
sicurezza e la privacy dei dati per
cliente Google Cloud, ti senta sicu
requisiti GDPR. Se collabori con G
conformità al GDPR:

1. Impegnarsi nei nostri contratti a rispettare il GDPR in relazione al nostro trattamento dei dati personali dei clienti in tutti i servizi Google Cloud Platform e Google Workspace
2. Offrendo funzionalità di sicurezza aggiuntive che possono aiutarti a proteggere meglio i dati personali più sensibili
3. Fornirti la documentazione e le risorse per assisterti nella valutazione della privacy dei nostri servizi
4. Continuare ad evolvere le nostre capacità man mano che il panorama normativo cambia

Impegni di Google Workspace e Google Cloud Platform rispetto al GDPR

I titolari del trattamento devono avvalersi di responsabili del trattamento con misure tecniche e organizzative adeguate. Quando conduci la tua valutazione GDPR di Google Cloud, considera quanto segue:

Espandi tutto

CONOSCENZA, AFFIDABILITÀ E RISORSE DI ESPERTI

Competenza nella protezione dei dati

Google impiega professionisti della s
massimi esperti mondiali di sicurezz
Questo team di esperti ha il compito

sviluppare processi di revisione della sicurezza, costruire infrastrutture di sicurezza più solide e implementare con precisione le politiche di sicurezza di Google.

Google si avvale inoltre di un ampio team di avvocati, esperti di conformità alle normative e specialisti delle politiche pubbliche che si occupano della conformità della privacy e della sicurezza per Google Cloud.

Questi team collaborano con clienti, parti interessate del settore e autorità di vigilanza per garantire che i nostri servizi Google Workspace e Google Cloud Platform possano aiutare i clienti a soddisfare le loro esigenze di conformità.

IMPEGNI IN MATERIA DI PROTEZIONE DEI DATI

Data Processing Agreements

Our data processing agreements for Google Workspace (https://workspace.google.com/terms/dpa_terms.html?uri=CELEX%3A32016R0679%3Futm_medium%3Det&%3Butm_source=google.com%2Fcloud&%3Butm_campaign=gdpr&%3Butm_content=commitments_to_the_gdpr&%3B_ga=2.254545160.1829542452.1518948405-1172296852.1493242673&hl=it) and Google Cloud Platform (https://cloud.google.com/terms/data-processing-terms?hl=it) clearly articulate our privacy commitment to customers. We have evolved these terms over the years based on feedback from our customers and regulators.

We specifically updated these terms to reflect the GDPR, and, to facilitate our customers' compliance assessment and GDPR readiness when using Google Cloud services. Learn more about the Google Workspace Data Processing Amendment (https://workspace.google.com/terms/dp… rd Contract Clauses (https://cloud.google.… Security Terms (https://cloud.google.com… Standard Contract Clauses (SCCs) (ht…

Our customers can enter into these u… s described for the Google Workspace …

(https://support.google.com/a/answer/2888485?hl=it) and the GCP Data Processing and Security Terms (https://support.google.com/cloud/answer/6329727?hl=it).

Processing According to Instructions

Any data that a customer and its users put into our systems will only be processed in accordance with the customer's instructions, as described in our GDPR-updated data processing agreements.

Personnel Confidentiality Commitments

All Google employees are required to sign a confidentiality agreement and complete mandatory confidentiality and privacy trainings, as well as our Code of Conduct training. Google's Code of Conduct specifically addresses responsibilities and expected behavior with respect to the protection of information.

UTILIZZO DI SUBPROCESSORI

Google Group companies directly conduct the majority of data processing activities required to provide the Google Workspace and Google Cloud Platform services. However, we do engage some third-party vendors to assist in supporting these services. Each vendor goes through a rigorous selection process to ensure it has the required technical expertise and can deliver the appropriate level of security and privacy.

We make information available about Google group subprocessors supporting Google Workspace (https://workspace.google.com/intl/en/terms/subprocessors.html?utm_medium=et&%3Butm_source=google.com%2Fcloud&%3Butm_campaign=gdpr&%3Butm_content=commitments_to_the_gdpr&%3B_ga=2.441...1172296852.1493242673&hl=it) and Google Cloud Platform (https://cl... well as third-party subprocessors inv... (https://workspace.google.com/intl/en/te... subprocessor details, and here (https:... subprocessor details. We also includ... processing agreements.

SICUREZZA DEI SERVIZI

According to the GDPR, appropriate technical and organisational measures shall be implemented to ensure a level of security appropriate to the risk.

Google operates a global infrastructure designed to provide state-of-the-art security through the entire information processing lifecycle. This infrastructure is built to provide secure deployment of services, secure storage of data with end-user privacy safeguards, secure communications between services, secure and private communication with customers over the Internet, and safe operation by administrators. Google Workspace and Google Cloud Platform run on this infrastructure.

We designed the security of our infrastructure in layers that build upon one another, from the physical security of data centers, to the security protections of our hardware and software, to the processes we use to support operational security. This layered protection creates a strong security foundation for everything we do. A detailed discussion of our Infrastructure Security can be found in Google Infrastructure Security Design Overview Whitepaper (https://cloud.google.com/security/infrastructure/design?hl=it).

Availability, Integrity & Resilience

Google designs the components of our platform to be highly redundant. Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products such as natural disasters and local outages. In the event of hardware, software, or network failure, services are automatically and instantly shifted from one facility to another so that operations can continue without interruption. Our highly redundant infrastructure helps customers protect themselves from data loss.

Equipment Testing and Security

Google utilizes barcodes and asset ta
equipment from acquisition to install
to pass a performance test at any po
retired. Google hard drives leverage t
drive locking, to protect data at rest.

Disaster Recovery Testing

Google conducts disaster recovery testing on an annual basis to provide a coordinated venue for infrastructure and application teams to test communication plans, fail-over scenarios, operational transition, and other emergency responses. All teams that participate in the disaster recovery exercise develop testing plans and post mortems which document the results and lessons learned from the tests.

Encryption

Google uses encryption to protect data in transit and at rest. Google Workspace data in transit between regions is protected using HTTPS, which is activated by default for all users. Google Workspace and Google Cloud Platform services encrypt customer content stored at rest, without any action required from customers, using one or more encryption mechanisms. A detailed discussion of how we encrypt data can be found in these resources: Workspace Encryption Whitepaper (https://services.google.com/fh/files/helpcenter/google_encryptionwp2016.pdf?utm_medium=et&%3Butm_source=google.com%2Fcloud&%3Butm_campaign=gdpr&%3Butm_content=commitments_to_the_gdpr%22&hl=it), and Google Cloud Encryption in transit (https://cloud.google.com/security/encryption-in-transit?hl=it) and at rest (https://cloud.google.com/security/encryption/default-encryption?hl=it).

Access Controls

For Google employees, access rights and levels are based on job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as dictated by Google's security policies. Data centers that house Google Cloud systems and infrastructure components are subjec 24 x 7 on-site security personnel, securit mechanisms, physical locks and vide facility.

Incident Management

Google has a dedicated security team responsible for security and privacy of customer data and managing security 24 hours a day and 7 days a week worldwide. Individuals from this team receive incident-related notifications and are responsible for helping resolve emergencies 24 x 7. Incident response policies are in place and procedures for resolving critical incidents are documented. Information from these events is used to help prevent future incidents and can be used as examples for information security training. Google incident management processes and response workflows are documented. Google's incident management processes are tested on a regular basis as part of our ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27001, PCI-DSS[1] (https://cloud.google.com/security/gdpr?hl=it#pci-dss-footnote), SOC 2 and FedRAMP programs to provide our customers and regulators with independent verification of our security, privacy, and compliance controls. More information on our incident response process can be found in our Data incident response process whitepaper (https://services.google.com/fh/files/misc/data_incident_response_2018.pdf?hl=it).

Vulnerability Management

We scan for software vulnerabilities using a combination of commercially available and purpose-built in-house tools, intensive automated and manual penetration testing, quality assurance processes, software security reviews, and external audits. We also rely on the broader security research community and greatly value their help identifying any vulnerabilities in Google Workspace, Google Cloud Platform, and other Google products. Our Vulnerability Reward Program encourages researchers to report design and implementation issues that may put customer data at risk.

Product Security: Google Workspace

Google Workspace customers can leverage product features and configurations to further protect personal data against unauthorised or unlawful processing:

Google Workspace Core Services (htt it), including Gmail, Google Admin Conso Hangouts, Chat, Meet, Cloud Search a lp ensure that your organization's data i unique requirements. 2-step verificati (https://support.google.com/a/answer/17 unauthorized access by asking users

in. Security key enforcement (https://www.youtube.com/watch?v=LUHOs_ggvi4&hl=it) offers another layer of security for user accounts by requiring a physical key. The Advanced Protection Program (https://landing.google.com/advancedprotection/?hl=it) is our strongest protection for users at risk of targeted online attacks. Suspicious Login Monitoring (https://support.google.com/a/answer/7102416?hl=it) detects suspicious logins using robust machine learning capabilities. Enhanced email security (https://support.google.com/a/answer/7280976?hl=it) requires email messages to be signed and encrypted using Secure/Multipurpose Internet Mail Extensions (S/MIME). Encryption (https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf?hl=it): Google Workspace customers' data is encrypted when it's on a disk, stored on backup media, moving over the Internet, or traveling between data centers. Data loss prevention (https://support.google.com/a/answer/6321530?hl=it) protects sensitive information within Gmail and Drive from unauthorized sharing. Advanced phishing and malware protection (https://support.google.com/a/answer/9157861?hl=it) protects against suspicious attachments and scripts from untrusted senders, as well as malicious links and images. Information rights management (https://www.youtube.com/watch?v=hdVVukQJWdA&hl=it) in Drive allows you to disable downloading, printing, and copying of files from the advanced sharing menu, and to set expiration dates on file access. Endpoint management (https://workspace.google.com/products/admin/endpoint/?hl=it) offers continuous system monitoring and alerts in case of suspicious device activity. Alert Center (https://workspace.google.com/products/admin/alert-center/?hl=it) is a place to view essential notifications, alerts, and actions across Google Workspace. Insights around these potential alerts can help administrators assess their organization's exposure to security issues. Security Center (https://workspace.google.com/products/admin/security-center/?hl=it) brings together security analytics, best practice recommendations and integrated remediation to protect your organization’s data, devices and users. It provides you with visibility into external file sharing, spam and malware targeting users within your organization, and integrated remediation via the investi

(https://support.google.com/a/answer/92

Google Workspace apps, based on a

(https://workspace.google.com/products/

your organization's email, Google Driv

eDiscovery and compliance needs. A

(https://support.google.com/a/answer/72

services using OAuth 2.0. Organizations can control which third-party and internal apps can access Google Workspace data, and find more details about any third-party apps already in use.Data Regions (https://workspace.google.com/products/admin/data-regions/?hl=it) lets you store your covered data in a specific geographic location by using a data region policy. Access Transparency (https://support.google.com/a/answer/9230474?hl=it) lets you review logs of actions taken by Google staff when accessing user content.

To learn more, please visit https://workspace.google.com/security (https://workspace.google.com/security?hl=it)

Product Security: GCP

GCP customers can leverage product features and configurations to further protect personal data against unauthorised or unlawful processing:

Encryption in transit between regions (https://cloud.google.com/security/encryption-in-transit?hl=it) is applied by default on GCP to encrypt requests before transmission and to protect the raw data using the Transport Layer Security (TLS) protocol. Once data is transferred to GCP to be stored, GCP applies encryption at rest (https://cloud.google.com/security/encryption/default-encryption?hl=it) by default.2-step verification (https://support.google.com/accounts/answer/6103523?hl=it#2-step_verification_methods) reduces the risk of unauthorized access by asking users for additional proof of identity when signing in. Security key enforcement (https://cloud.google.com/security-key?hl=it) offers another layer of security for user accounts by requiring a physical key.Cloud Identity and Access Management (Cloud IAM) (https://cloud.google.com/iam/docs?hl=it) allows you to create and manage fine-grained access and modification permissions for Google Cloud Platform resources.Data Loss Prevention API (https://cloud.google.com/dlp?hl=it) helps to identify and monitor the processing of special categories of personal data in order to implement adequate controls.Cloud Logging (htt ing (https://cloud.google.com/monitoring?hl= aly detection systems into Google Cloud (https://cloud.google.com/iap?hl=it) (Clo ng on Google Cloud Platform.Cloud Secu (https://cloud.google.com/security-scann es in Google App Engine applications.VP

(https://cloud.google.com/vpc-service-controls?hl=it) provide perimeter protection for services that store highly sensitive data to enable service-level data segmentation.Cloud KMS (https://cloud.google.com/security-key-management?hl=it) and HSM (https://cloud.google.com/kms/docs/hsm?hl=it) allow for management of encryption keys and cryptographic operations from within a cluster of FIPS 140-2 Level 3 certified Hardware Security Modules (HSMs). KMS allows customers to use Google-managed or customer-managed encryption keys as required to fulfill compliance requirements.Cloud Security Command Center (https://cloud.google.com/security-command-center?hl=it) allows customers to view and monitor an inventory of their cloud assets, scan storage systems for sensitive data, detect common web vulnerabilities, and review access rights to their critical resources from a single, centralized dashboard.Access Approval (https://cloud.google.com/cloud-provider-access-management/access-approval/docs?hl=it) requires Google administrators to seek explicit customer approval before Google can access data. It 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.

To learn more, please visit https://cloud.google.com/security/ (https://cloud.google.com/security?hl=it)

[1] For Google Cloud Platform only.

CONSERVAZIONE E CANCELLAZIONE DEI DATI

Administrators can export customer data, via the functionality of the Google Workspace (https://support.google.com/accounts/answer/3024190?hl=it) or Google Cloud Platform services (consult Google Cloud Platform docu
further information), at any time durir
export commitments in our data proc
work to enhance our data export capa
copy of your customer data from Goo
(https://workspaceupdates.googleblog.co
Google Cloud Platform services.

You can also delete customer data, via the functionality of the Google Workspace or Google Cloud Platform services, at any time. When Google receives a complete deletion instruction from you (such as when an email you have deleted can no longer be recovered from your “trash”), Google will delete the relevant customer data from all of its systems within a maximum period of 180 days unless retention obligations apply.

ASSISTENZA AL TITOLARE

Data Subject's Rights

Data controllers can use the Google Workspace and Google Cloud Platform administrative consoles and services functionality to help access, rectify, restrict the processing of, or delete any data that they and their users put into our systems. This functionality will help them fulfill their obligations to respond to requests from data subjects to exercise their rights under the GDPR.

Data Protection Team

Google has designated a DPO for Google LLC and its subsidiaries, to cover data processing subject to the GDPR, including as part of our Cloud products and services. Emil Ochotta is Google's Data Protection Officer. Dr. Ochotta is based in Sunnyvale in the U.S.

Where required, Google Cloud products have designated teams to address customer inquiries in relation to data protection. The way to contact these teams is described in the relevant agreement. For Google Workspace the Cloud Data Protection Team can be contacted by Customer’s administrators at https://support.google.com/a/contact/googlecloud_dpr (https://support.google.com/a/contact/g in to their admin account) and/or direct e applicable agreement. For Google Cl at https://support.google.com/cloud/ (https://support.google.com/cloud/conta

Incident Notifications

Google Workspace and Google Cloud Platform have provided contractual commitments around incident notification for many years. We will continue to promptly inform you of incidents involving your customer data in line with the data incident terms in our current agreements.

TRASFERIMENTI INTERNAZIONALI DI DATI

The GDPR provides for several mechanisms to facilitate transfers of personal data outside of the EU. These mechanisms are aimed at confirming an adequate level of protection or ensuring the implementation of appropriate safeguards when personal data is transferred to a third country.

An adequate level of protection can be confirmed by adequacy decisions such as the ones that support the Japanese Act on the Protection of Personal Information (APPI) and the Swiss Data Protection Act.

Where personal data will be transferred outside of the EU to third countries not covered by adequacy decisions, we commit under our data processing agreements to maintain a mechanism that will facilitate these transfers as required by the GDPR. In 2017, we gained confirmation of compliance from European Data Protection Authorities for our standard contract clauses, affirming that our contractual commitments for Google Workspace and Google Cloud Platform met the requirements to legally frame transfers of personal data from the EU to the third countries that do not provide adequate protection.

Safeguards for International Data Transfers with Google Cloud
(https://services.google.com/fh/gumdrop/preview/misc/safeguards_for_international_data_transfers_with_google_cloud.pdf?hl=it)

Safeguards for International Data Tr... for Education
(https://services.google.com/fh/files/mis...tion al_data_transfers.pdf?hl=it)

NORME E CERTIFICAZIONI

Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google Workspace and Google Cloud Platform undergo several independent third-party audits on a regular basis to provide this assurance.

ISO/IEC 27001 (Information Security Management)

ISO/IEC 27001 is one of the most widely recognized, internationally accepted independent security standards. Google has earned ISO/IEC 27001 certification for the systems, applications, people, technology, processes, and data centers that make up our shared Common Infrastructure (https://services.google.com/fh/files/misc/2018_google_common_infrastructure_iso_27001.pdf?hl=it) as well as for Google Workspace and Google Cloud Platform products. You can access these certificates via Compliance reports manager (https://cloud.google.com/security/compliance/compliance-reports-manager?hl=it).

ISO/IEC 27017 (Cloud Security)

ISO/IEC 27017 is an international standard of practice for information security controls based on ISO/IEC 27002, specifically for Cloud Services. Google has been certified compliant with ISO/IEC 27017 for Google Workspace and Google Cloud Platform. You can access these certificates via Compliance reports manager (https://cloud.google.com/security/compliance/compliance-reports-manager?hl=it).

ISO/IEC 27018 (Cloud Privacy)

ISO/IEC 27018 is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services. Google has been certified compliant with ISO/IEC 27018 for Google Workspace and Google Cloud Platform. You can access these certificates via Compliance reports manager (https://cloud.google.com/security/compliance/compliance-reports-manager?hl=it).

ISO/IEC 27701 (Privacy Information M

ISO/IEC 27701 is a global privacy sta g of personally identifiable information (P EC 27001 and ISO/IEC 27002 to include 27701 certification as a PII processor

Platform. You can access these certificates via Compliance reports manager (https://cloud.google.com/security/compliance/compliance-reports-manager?hl=it).

SSAE18/ISAE 3402 (SOC 2/3)

The American Institute of Certified Public Accountants (AICPA) SOC 2 (Service Organization Controls) and SOC 3 audit framework defines Trust Principles and criteria for security, availability, processing integrity, and confidentiality. Google has both SOC 2 and SOC 3 reports for Google Workspace and Google Cloud Platform. You can access these certificates via Compliance reports manager (https://cloud.google.com/security/compliance/compliance-reports-manager?hl=it).

Valutazione di Google Cloud in base all'articolo 28

L'articolo 28 del GDPR stabilisce i requisiti di un responsabile del trattamento che tratta i dati per conto del titolare del trattamento. Scopri come i nostri termini riflettono questi requisiti.

Espandi tutto

Utilizzo di sub-responsabili

GCP - Termini per l'elaborazione e la sicurezza dei dati (DPST)

Definizioni | Sezione 2.1 (https://cloud.google.com/terms/data-processing-terms?hl=it#2.-definitions)

Sicurezza dei dati | Sezione 7.1.2 (https://cloud.google.com/terms/data-pro

Sicurezza dei dati | Sezione 7.3.1 (b) (https://cloud.google.com/terms/data-pro

Trasferimenti di dati | Sezione 10.1 (https://cloud.google.com/terms/data-pro

Subincaricati | Sezione 11
(https://cloud.google.com/terms/data-processing-terms?hl=it#11.-subprocessors)

Terzo Beneficiario | Sezione 14
(https://cloud.google.com/terms/data-processing-terms?hl=it#14.-third-party-beneficiary)

Appendice 2.1–2.5
(https://cloud.google.com/terms/data-processing-terms?hl=it#appendix-2:-security-measures)

GCP - Clausole contrattuali standard dell'UE (SCC)

SCC (da titolare a responsabile del trattamento dell'UE)
(https://cloud.google.com/terms/sccs/eu-c2p?hl=it) | Allegato II, Allegato III

SCC (da responsabile del trattamento a responsabile del trattamento dell'UE)
(https://cloud.google.com/terms/sccs/eu-p2c?hl=it) | N / A

SCC (da responsabile del trattamento a responsabile del trattamento dell'UE)
(https://cloud.google.com/terms/sccs/eu-p2p?hl=it) | Allegato II, Allegato III

SCC (da processore a responsabile del trattamento dell'UE, esportatore di Google)
(https://cloud.google.com/terms/sccs/eu-p2p-intra-group?hl=it) | Allegato II, Allegato III

SCC (da controller a responsabile del trattamento del Regno Unito)
(https://cloud.google.com/terms/sccs/uk-c2p?hl=it) | Clausola 1, Clausola 3.3, Clausola 4 (g) e (i), Clausola 5 (i) e (j), Clausola 6, Clausola 8, Clausola 11, Clausola 12, Appendice 1, Appendice 2.5

Contenuti correlati: Subprocessori GCP (https://cloud.google.com/terms/subprocessors?hl=it)

GOOGLE WORKSPACE - Termini per il trattamento dei dati

Definizioni | Sezione 2.1 (https://works

Sicurezza dei dati | Sezione 7.1.2
(https://workspace.google.com/terms/dp

Sicurezza dei dati | Sezione 7.3.1 (b)
(https://workspace.google.com/terms/dp

Trasferimenti di dati | Sezione 10.1
(https://workspace.google.com/terms/dpa_terms.html?hl=it#10-data-transfers)

Subincaricati | Sezione 11
(https://workspace.google.com/terms/dpa_terms.html?hl=it#11-subprocessors)

Terzo Beneficiario | Sezione 14
(https://workspace.google.com/terms/dpa_terms.html?hl=it#14-third-party-beneficiary)

Misure di sicurezza | Appendice 2.1–2.5
(https://workspace.google.com/terms/dpa_terms.html?hl=it#appendix-2)

GOOGLE WORKSPACE - Clausole contrattuali standard dell'UE (SCC)

SCC (da titolare a responsabile del trattamento dell'UE)
(https://cloud.google.com/terms/sccs/eu-c2p?hl=it) | Allegato II, Allegato III

SCC (da responsabile del trattamento a responsabile del trattamento dell'UE)
(https://cloud.google.com/terms/sccs/eu-p2c?hl=it) | N / A

SCC (da responsabile del trattamento a responsabile del trattamento dell'UE)
(https://cloud.google.com/terms/sccs/eu-p2p?hl=it) | Allegato II, Allegato III

SCC (da processore a responsabile del trattamento dell'UE, esportatore di Google)
(https://cloud.google.com/terms/sccs/eu-p2p-intra-group?hl=it) | Allegato II, Allegato III

SCC (da controller a responsabile del trattamento del Regno Unito)
(https://cloud.google.com/terms/sccs/uk-c2p?hl=it) | Clausola 1, Clausola 3.3, Clausola 4 (g) e (i), Clausola 5 (i) e (j), Clausola 6, Clausola 8, Clausola 11, Clausola 12, Appendice 1, Appendice 2.5

Contenuti correlati: Contratto per i su'
(https://workspace.google.com/intl/en/te

Contratto scritto generale

GCP - Data Processing and Security Terms (DPST)

Entire Data Processing and Security Terms

(https://cloud.google.com/terms/data-processing-terms?hl=it)

GOOGLE WORKSPACE- Data Processing Terms

(https://workspace.google.com/terms/dpa_terms.html?hl=it)

Entire Data Processing Terms (https://workspace.google.com/terms/dpa_terms.html?hl=it)

Elaborazione secondo istruzioni documentate

GCP - Data Processing and Security Terms (DPST)

Processing of Data | Section 5.2

(https://cloud.google.com/terms/data-processing-terms?hl=it#5.-processing-of-data)

GCP - EU Standard Contract Clauses (SCC)

SCCs (http://cloud.google.com/terms/sccs?hl=it)

GOOGLE WORKSPACE - Data Processing Terms

Section 5.2 | Processing of Data

(https://workspace.google.com/terms/dpa_terms.html?hl=it#5-processing-of-data)

GOOGLE WORKSPACE - EU Standard Contract Clauses (SCC)

Clause 5 (a) and (b) | Obligations of the Data Importer

(https://workspace.google.com/terms/mcc terms.html?hl=it#clause-5)

Trattamento in base agli obb

GCP - Google Cloud Platform Terms o

Confidential Information |Section 7 (

GCP -Data Processing and Security Terms (DPST)

Data Security | Section 7.1.2

(https://cloud.google.com/terms/data-processing-terms?hl=it#7.-data-security)

Data Security | Section 7.5.3

(https://cloud.google.com/terms/data-processing-terms?hl=it#7.-data-security)

Personnel Security | Appendix 2.4

(https://cloud.google.com/terms/data-processing-terms?hl=it#appendix-2:-security-measures)

GCP - EU Standard Contract Clauses (SCC)

Obligations of the Data Importer | Clause 5

(https://cloud.google.com/terms/eu-model-contract-clause?hl=it#clause5)

GOOGLE WORKSPACE - Google Workspace Agreement

Confidential Information | Section 6

(https://workspace.google.com/intl/en_uk/terms/2013/1/premier_terms.html?hl=it)

GOOGLE WORKSPACE - Data Processing Terms

Data Security | Section 7.1.2

(https://workspace.google.com/terms/dpa_terms.html?hl=it#7-data-security)

Data Security | Section 7.5.3

(https://workspace.google.com/terms/dpa_terms.html?hl=it#7-data-security)

Personnel Security | Appendix 2.4

(https://workspace.google.com/terms/dpa_terms.html?hl=it#appendix-2-4-personnel-security)

GOOGLE WORKSPACE - EU Standard C

SCCs (http://cloud.google.com/terms/sc

Misure di sicurezza

GCP - Data Processing and Security Terms (DPST)

Data Security | Section 7

(https://cloud.google.com/terms/data-processing-terms?hl=it#7.-data-security)

Security Measures | Appendix 2

(https://cloud.google.com/terms/data-processing-terms?hl=it#appendix-2:-security-measures)

GCP - EU Standard Contract Clauses (SCC)

SCCs (http://cloud.google.com/terms/sccs?hl=it)

GOOGLE WORKSPACE - Data Processing Terms

Data Security | Section 7

(https://workspace.google.com/terms/dpa_terms.html?hl=it#7-data-security)

Security Measures | Appendix 2

(https://workspace.google.com/terms/dpa_terms.html?hl=it#appendix-2)

GOOGLE WORKSPACE - EU Standard Contract Clauses (SCC)

SCCs (http://cloud.google.com/terms/sccs?hl=it)

Related contentGoogle Cloud Security & Compliance Whitepaper

(https://static.googleusercontent.com/media/gsuite.google.com/en//files/google-apps-security-and-compliance-whitepaper.pdf)

Assistance to Data Controller

GCP - Data Processing and Security T

Impact Assessments and Consultatio

(https://cloud.google.com/terms/data-pro
consultations)

GOOGLE WORKSPACE - Data Process

Impact Assessments and Consultations | Section 8

(https://workspace.google.com/terms/dpa_terms.html?hl=it#8-impact-assessments-and-consultations)

Data Deletion and Data Return

GCP - Data Processing and Security Terms (DPST)

Data Deletion | Section 6

(https://cloud.google.com/terms/data-processing-terms?hl=it#6.-data-deletion)

Data Subject Rights; Data Export | Section 9.1

(https://cloud.google.com/terms/data-processing-terms?hl=it#9.-access-etc.;-data-subject-rights;-data-export)

GCP - EU Standard Contract Clauses (SCC)

SCCs (http://cloud.google.com/terms/sccs?hl=it)

GOOGLE WORKSPACE- Data Processing Terms

Data Deletion |Section 6

(https://workspace.google.com/terms/dpa_terms.html?hl=it#6-data-deletion)

Data Subject Rights; Data Export | Section 9.1

(https://workspace.google.com/terms/dpa_terms.html?hl=it#9-data-subject-rights-data-export)

GOOGLE WORKSPACE- EU Standard Contract Clauses (SCC)

SCCs (http://cloud.google.com/terms/sccs?hl=it)

Demonstrate Compliance

GCP - Data Processing and Security T

Data Security | Section 7.4

(https://cloud.google.com/terms/data-pro

Related content: Google Cloud Compliance

(https://www.google.com/cloud/security/compliance/?hl=it)

GOOGLE WORKSPACE - Data Processing Terms

Data Security | Section 7.4

(https://workspace.google.com/terms/dpa_terms.html?hl=it#7-data-security)

Related content: Google Cloud Compliance

(https://www.google.com/cloud/security/compliance/?hl=it)

Relevant Whitepapers

Read our whitepapers relevant to Google Cloud customers who are subject to GDPR

Google Workspace Data Protection Implementation Guide

Data Protection in Workspace

Google Workspace For Ed Implementation Guide

Data Protection in Workspace for

Trusting Google Cloud Platform With Your Data

Data Protection in Google Cloud Platform

Safeguards For International Data Transfers With Google Cloud

Cross Border Transfers in Google Cloud

FAQ

Answers to Frequently Asked Questions about Google Cloud and GDPR

Espandi tutto

Does the GDPR require storage of personal data in the EU?

No. Like the 95/46/EC Directive on D
(https://eur-lex.europa.eu/legal-content/E
utm_medium=et&utm_source=google.con
, the GDPR sets out certain condition
Such conditions can be met via mech

How do your terms reflect th

For many years, Google Cloud has offered data processing terms that clearly articulate our privacy and security commitment to customers, and we have evolved those terms to reflect the GDPR. Our GDPR-updated terms notably reflect the provisions of Article 28 of the GDPR governing the use of a data processor by a data controller.

Does the GDPR give customers the right to audit Google Cloud?

Under the GDPR, audit rights must be granted to data controllers in their contracts with data processors. Our updated data processing agreements include audit rights for the benefit of customers who are subject to the GDPR.

What role do third-party ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701 and SOC 2/3 reports play in compliance with the GDPR?

Our third-party ISO/IEC certifications and SOC 2/3 audit reports can be used by customers to help conduct their risk assessments and help them determine whether appropriate technical and organisational measures are in place. Our ISO/IEC 27701 certification provides greater clarity on privacy-related roles and responsibilities, which can facilitate efforts to comply with privacy regulations, including the GDPR.

How does Google Cloud support International Data Transfers in the Cloud?

The GDPR provides for several mech
of the EU. These mechanisms are air
ensuring the implementation of appr
to a third country.

An adequate level of protection can b
that support the Japanese Act on the
(https://cloud.google.com/security/comp
Act.

Where personal data will be transferred outside of the EU to third countries not covered by adequacy decisions, we commit under our data processing agreements to maintain a mechanism that will facilitate these transfers as required by the GDPR. In 2017, we gained confirmation of compliance from European Data Protection Authorities for our standard contract clauses, affirming that our contractual commitments for Google Workspace and Google Cloud Platform met the requirements to legally frame transfers of personal data from the EU to the third countries that do not provide adequate protection.

Now that Privacy Shield has been invalidated, can I still use Google Cloud and meet GDPR requirements if I handle EU personal data?

While Google will continue to review the impact of the Court of Justice of the European Union (CJEU) case C-311/18 one thing remains unchanged: Google will take appropriate steps to ensure we maintain a high level of privacy protection for EU citizens.

Google Cloud offers Standard Contractual Clauses (SCCs) to our customers, which will be automatically deemed to apply in the absence of any alternate transfer solution made available by Google. Regardless of the location of the data, data protection remains a priority for Google. See the Safeguards for International Data Transfers with Google Cloud Whitepaper (https://services.google.com/fh/files/misc/safeguards_for_international_data_transfers_with_google_cloud.pdf?hl=it) for more information.

We are certified against recognised international standards such as ISO/IEC 27001 (https://cloud.google.com/security/compliance/iso-27001?hl=it), ISO/IEC 27018 (https://cloud.google.com/security/compliance/iso-27018?hl=it) and ISO/IEC 27017 (https://cloud.google.com/security/compliance/iso-27017?hl=it). The complete listing of Google's compliance offerings can be found on the compliance resource center (https://cloud.google.com/security/compliance?hl=it).

What other information and GDPR?

Refer to Google's Cloud's Privacy Res ...nd Google's Businesses and Data websi...

(https://privacy.google.com/businesses/?uri=CELEX%3A31995L0046&%3Bfrom=EN%3Futm_medium%3Det&%3Butm_source=google.com%2Fcloud&%3Butm_campaign=gdpr&%3Butm_content=gdpr_faqs&hl=it)

.

Where can I find other European Privacy Resources?

Refer to our European Compliance offerings (https://cloud.google.com/security/compliance/offerings?hl=it#/regions=EMEA&focusArea=Privacy) and the Cloud Privacy Resource Center (https://cloud.google.com/privacy/?hl=it).

Disclaimer: The content contained herein is correct as of August 2021 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers. When referring to Google Workspace, we also refer to Google Workspace for Education. We are bringing Google Workspace to our education and nonprofit customers in the coming months.

Take the next step

Start building on Google Cloud with $300 in free credits and 20+ always free products.

Get started for free (https://console.cloud.google.com/freetrial?hl=it)

Need help getting started?

Contact sales (https://cloud.google

Work with a trusted partner

Find a partner (https://cloud.withg

Continue browsing

See all products (https://cloud.google.com/products/?hl=it)