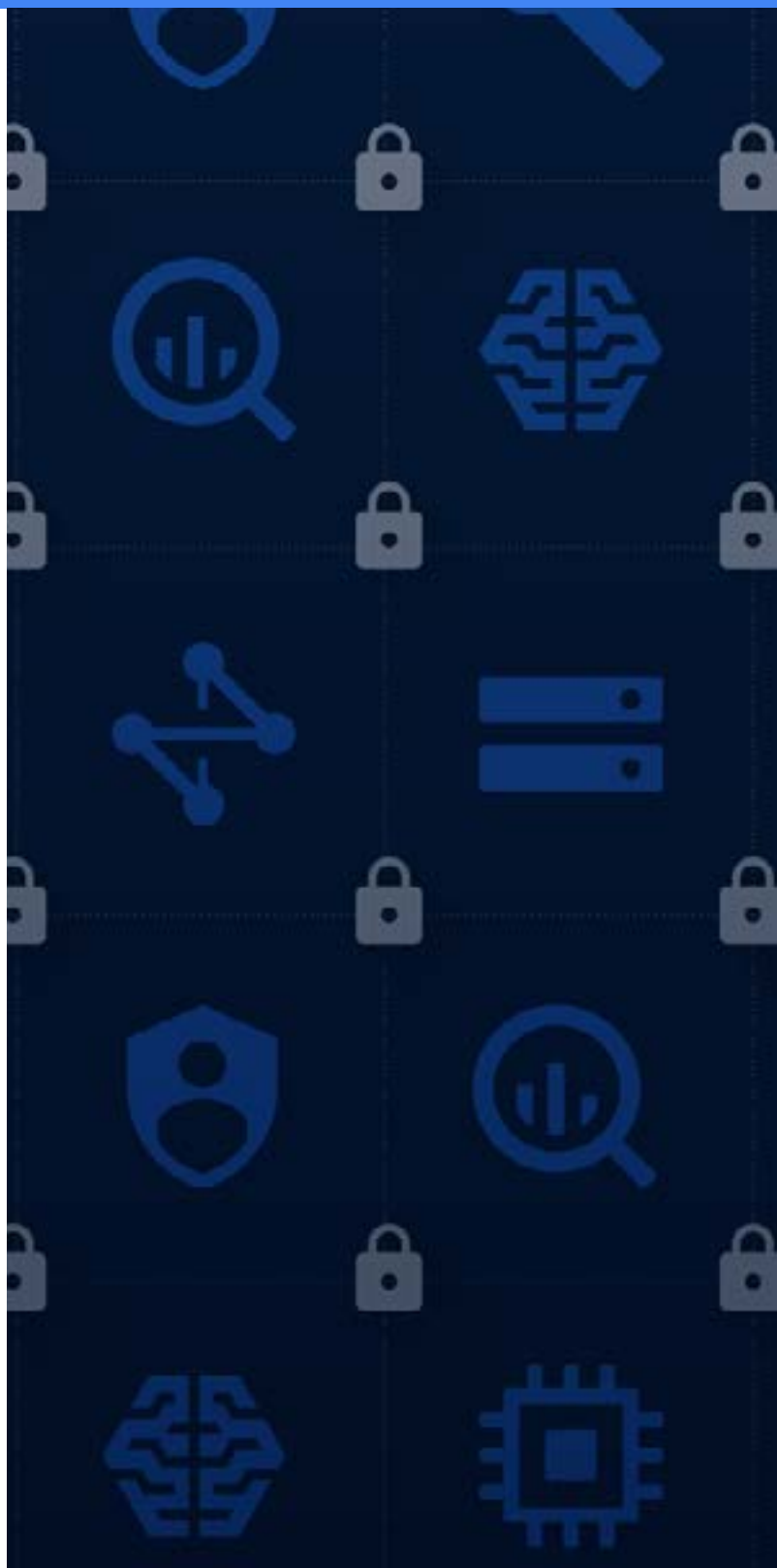
Google Cloud

Google Cloud e la General Data Protection Regulation (GDPR)



INTRODUZIONE

Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation)

Il 25 maggio 2018 entrerà in vigore la normativa europea più importante degli ultimi 20 anni per quel che riguarda la protezione dei dati. Il regolamento EU General Data Protection Regulation (GDPR) va a sostituire la 1995 EU Data Protection Directive. Il regolamento GDPR rafforza i diritti delle persone riguardo ai propri dati personali e mira a unificare le leggi sulla protezione dei dati dei vari paesi europei, a prescindere da dove vengano elaborati i dati.

Google garantisce che rispetterà fedelmente il regolamento GDPR nei servizi di Google Cloud. Ci impegniamo inoltre a sostenere i nostri clienti nelle attività di conformità al regolamento GDPR fornendo strumenti efficaci di protezione della privacy e della sicurezza, peraltro già incorporati nei nostri servizi e contratti nel corso degli anni.

COSA PUOI FARE

Quali sono le tue responsabilità in qualità di cliente?

I clienti di G Suite[1] e Google Cloud Platform di solito sono i responsabili del trattamento di tutti i dati personali che forniscono a Google e che riguardano l'uso dei servizi Google. Il responsabile del trattamento dei dati determina gli scopi e i mezzi per l'elaborazione dei dati personali, mentre il responsabile dell'elaborazione dei dati elabora i dati per conto del responsabile del trattamento dei dati. Google è un'azienda responsabile dell'elaborazione dei dati, pertanto gestisce i dati personali per conto del responsabile del trattamento dei dati che utilizza G Suite o Google Cloud Platform. I responsabili del trattamento dei dati devono implementare misure tecniche e organizzative adeguate per garantire e dimostrare che l'elaborazione dei dati viene eseguita in conformità al regolamento GDPR. Gli obblighi dei responsabili del trattamento dei dati riguardano vari aspetti quali legittimità, correttezza, trasparenza, limitazione delle finalità, riduzione al minimo dei dati, accuratezza e rispetto dei diritti dei proprietari dei dati.

I responsabili del trattamento dei dati potrebbero trovare informazioni utili riguardo il proprio ruolo secondo i termini del regolamento GDPR controllando regolarmente il sito web dell'ente nazionale o responsabile della protezione dei dati indicato nel regolamento GDPR (secondo i casi)[2], nonché consultando le pubblicazioni di associazioni che si occupano della privacy dei dati, ad esempio l'**International Association of Privacy Professionals (IAPP).**

Dovresti inoltre rivolgerti a consulenti legali indipendenti per conoscere il tuo stato e gli obblighi previsti dal regolamento GDPR, dato che solo un avvocato può fornire informazioni legali specifiche per la tua situazione. Tieni presente che le informazioni in questo sito web non forniscono indicazioni legali né sostituiscono la consulenza di un avvocato.

Da dove iniziare

In qualità di cliente attuale o potenziale di Google Cloud, ti conviene prepararti per quando il regolamento GDPR entrerà in vigore. Ecco qualche consiglio.

- Inizia a studiare le disposizioni del regolamento **GDPR**, in particolare le differenze rispetto agli obblighi attuali per la protezione dei dati.
- Considera la possibilità di creare un inventario aggiornato dei dati personali che gestisci. Puoi utilizzare alcuni dei nostri strumenti per identificare e classificare i dati.
- Rivedi i tuoi controlli, criteri e processi attuali per stabilire se rispettano i requisiti del regolamento GDPR e sviluppa un piano per far fronte a eventuali lacune.
- Cerca di capire in che modo puoi sfruttare le funzioni esistenti di Google Cloud per la protezione dei dati nell'ambito del processo di adeguamento al quadro normativo. Esamina i materiali di revisione e certificazione di terze parti relativi a G Suite o Google Cloud Platform per stabilire in che modo possono esserti di aiuto in questa operazione.
- Tieni sotto controllo i nuovi orientamenti normativi non appena diventano disponibili e consulta un avvocato per ottenere consigli legali specifici per la tua azienda.

1 G Suite include G Suite for Business e G Suite for Education.

2 Ti consigliamo di richiedere assistenza legale indipendente per individuare l'ente nazionale o incaricato ufficialmente della protezione dei dati.

COSA STIAMO FACENDO

G Suite e Google Cloud Platform - I nostri impegni per rispettare il regolamento GDPR

Tra le altre cose, i responsabili del trattamento dei dati devono utilizzare esclusivamente responsabili dell'elaborazione dei dati che forniscano garanzie sufficienti per implementare misure tecniche e organizzative adeguate in modo che l'elaborazione rispetti i requisiti del regolamento GDPR. Ecco alcuni aspetti da prendere in considerazione al momento di valutare i servizi G Suite e Google Cloud Platform.

CONOSCENZE DEGLI ESPERTI, AFFIDABILITÀ E RISORSE

Esperienza nella protezione dei dati

Per Google lavorano vari professionisti della sicurezza e della privacy, tra cui alcuni dei maggiori esperti mondiali nel campo della protezione delle informazioni, delle applicazioni e delle reti. Questo team si occupa di gestire i nostri sistemi di difesa, sviluppare processi mirati al controllo della sicurezza, creare un'infrastruttura di sicurezza e implementare i criteri di Google relativi alla sicurezza.

Inoltre, Google si avvale di un ampio team di professionisti legali, esperti di conformità alle normative e specialisti di politiche pubbliche che gestiscono la conformità alle leggi su privacy e sicurezza da parte di Google.

Questi team interagiscono con clienti, parti interessate nel settore ed enti di supervisione per creare servizi G Suite *e* Google Cloud Platform *che consentano ai nostri clienti di far fronte ai propri requisiti di conformità.*

IMPEGNI PER LA PROTEZIONE DEI DATI

Contratti per l'elaborazione dei dati (Data Processing Agreement, DPA)

I nostri accordi contrattuali sull'elaborazione dei dati per G Suite e Google Cloud Platform descrivono chiaramente il nostro impegno nel garantire il rispetto della privacy dei nostri clienti. Nel corso degli anni, abbiamo aggiornato questi termini in base ai feedback dei nostri clienti e degli enti normativi.

Recentemente abbiamo aggiornato questi termini specificamente per riflettere il regolamento GDPR e abbiamo reso disponibili tali aggiornamenti con largo anticipo prima della sua entrata in vigore, per facilitare i nostri clienti nella valutazione del loro adempimento e nella preparazione al regolamento GDPR al momento dell'utilizzo dei servizi di Google Cloud. I nostri clienti possono aderire a questi termini aggiornati sull'elaborazione dei dati attraverso la procedura di adesione descritta qui per l'Emendamento sull'elaborazione dei dati di G Suite e qui per i Termini per l'elaborazione e la sicurezza dei dati di GCP. I termini aggiornati saranno validi a partire dal 25 maggio 2018, con l'entrata in vigore del regolamento GDPR.

Istruzioni specifiche di elaborazione

I dati che un cliente e i suoi utenti immettono nei nostri sistemi verranno elaborati esclusivamente in conformità con le istruzioni del cliente, come descritto nei nostri contratti per l'elaborazione dei dati attuali e in quelli aggiornati secondo il regolamento GDPR.

Rispetto della riservatezza da parte del personale

Tutti i dipendenti Google devono firmare un accordo di riservatezza e completare i corsi di formazione obbligatori su riservatezza e privacy, nonché il nostro corso di formazione relativo al ***Codice di condotta****. Il Codice di condotta di Google identifica in modo specifico le responsabilità e il comportamento previsto per quel che riguarda la protezione delle informazioni.*

USO DI SUB-RESPONSABILI

Le società del gruppo Google svolgono direttamente la maggior parte delle attività di elaborazione dei dati necessari per fornire i servizi di G Suite e Google Cloud Platform. Tuttavia, ci rivolgiamo anche ad alcuni fornitori esterni che ci aiutano a supportare questi servizi. Ogni fornitore deve superare un rigoroso processo di selezione mirato a garantirne le competenze tecniche e la capacità di offrire il livello adeguato di sicurezza e privacy. Rendiamo disponibili le informazioni sui sub-responsabili dell'elaborazione dei dati appartenenti al gruppo Google a supporto dei servizi G Suite e Google Cloud Platform, nonché su quelli terzi coinvolti in tali servizi, e includiamo impegni relativi ai sub-responsabili negli accordi, attuali e aggiornati, sull'elaborazione dei dati.

SICUREZZA DEI SERVIZI

Secondo il regolamento GDPR, il responsabile del trattamento dei dati e il responsabile dell'elaborazione dei dati devono implementare misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio. Google gestisce un'infrastruttura globale progettata per fornire una sicurezza all'avanguardia durante tutto il ciclo di vita dell'elaborazione delle informazioni. Questa infrastruttura garantisce quanto segue: implementazione sicura dei servizi, archiviazione sicura dei dati con misure protettive per la privacy degli utenti finali, comunicazioni protette tra i vari servizi, comunicazioni protette e private con i clienti su Internet e gestione sicura da parte degli amministratori. G Suite e Google Cloud Platform vengono eseguiti su questa infrastruttura. La sicurezza della nostra infrastruttura è progettata in vari livelli sovrapposti, da quella fisica dei data center a quella per le nostre risorse hardware e software, fino ai processi utilizzati per supportare la sicurezza operativa. Questa protezione "multistrato" è alla base di tutte le nostre operazioni. Puoi trovare informazioni dettagliate sulla sicurezza della nostra infrastruttura nel nostro **whitepaper sulla panoramica della progettazione della sicurezza per l'infrastruttura Google.**

Disponibilità, integrità e resilienza

Google progetta i componenti della propria piattaforma in modo che abbiano una ridondanza elevata. I data center di Google sono distribuiti geograficamente in modo da ridurre al minimo l'impatto di eventuali problemi a livello locale, ad esempio disastri naturali e interruzioni del servizio, sui prodotti globali. In caso di guasti all'hardware, al software o alla rete, i servizi vengono spostati automaticamente e immediatamente da una struttura fisica a un'altra, in modo che le operazioni possano continuare senza interruzioni. Grazie all'elevata ridondanza della nostra infrastruttura, i clienti sono protetti da possibili perdite di dati.

Test

Google esegue annualmente una serie di test relativi al ripristino di emergenza. Ciò consente ai team dell'infrastruttura e delle applicazioni di coordinare le attività mirate a testare piani di comunicazione, scenari di failover, transizione operativa e altre misure in caso di emergenza. Tutti i team che partecipano alle operazioni per il ripristino di emergenza sviluppano piani di test e analisi post mortem per documentare le informazioni e i risultati ottenuti dai test.

Crittografia

Google utilizza la crittografia per proteggere i dati sia in transito sia permanenti. Quelli che passano in G Suite sono protetti mediante il protocollo HTTPS, attivato per impostazione predefinita per tutti gli utenti. I servizi di G Suite e Google Cloud Platform utilizzano uno o più meccanismi di crittografia per criptare i contenuti dei clienti che vengono memorizzati al loro interno, senza che sia richiesta alcuna azione da parte dei clienti. Per informazioni dettagliate sulla crittografia dei dati, consulta il nostro **whitepaper sulla crittografia**.

Controlli dell'accesso

I diritti e i livelli di accesso dei dipendenti Google si basano sulla mansione e sul ruolo lavorativo che hanno, utilizzando i principi del "least-privilege" e "need-to-know", in funzione delle responsabilità definite per il dipendente. Le richieste di ulteriore accesso seguono un processo formale che prevede l'approvazione da parte del proprietario dei dati o del sistema oppure da parte di responsabili o altri dirigenti, a seconda dei criteri di sicurezza stabiliti da Google.

Gestione delle vulnerabilità

Per rilevare eventuali vulnerabilità software, utilizziamo una combinazione di strumenti sia disponibili in commercio sia sviluppati internamente e specificatamente, nonché test automatici e manuali per verificare possibili violazioni, processi di controllo della qualità, analisi della sicurezza del software e audit esterni. Ci affidiamo anche alla più ampia comunità di esperti della sicurezza, il cui aiuto è estremamente utile per identificare le vulnerabilità in G Suite, Google Cloud Platform e altri prodotti Google. Il nostro Vulnerability Reward Program (programma a premi per il rilevamento delle vulnerabilità) incoraggia gli esperti della sicurezza a segnalare i problemi di progettazione e implementazione che potrebbero mettere a rischio i dati dei clienti.

Sicurezza dei prodotti: G Suite

I clienti di G Suite possono sfruttare le funzioni e le configurazioni del prodotto per proteggere ulteriormente i dati personali da possibili elaborazioni non autorizzate o illegali.

- *La verifica in due passaggi riduce sensibilmente il rischio di accessi non autorizzati mediante la richiesta di ulteriori prove dell'identità degli utenti che accedono. L'applicazione delle chiavi di sicurezza fornisce un livello aggiuntivo di protezione per gli account utente mediante la richiesta di una chiave fisica.*
- *Il monitoraggio degli accessi sospetti consente di rilevare possibili intrusioni mediante funzioni di machine learning molto solide.*
- *La sicurezza avanzata per le email prevede che i messaggi email siano firmati e crittografati mediante estensioni S/MIME (Secure/Multipurpose Internet Mail Extension).*
- *Le funzioni di prevenzione della perdita dei dati impediscono che le informazioni sensibili all'interno di Gmail e Drive vengano condivise senza autorizzazione. Puoi trovare ulteriori informazioni nel nostro whitepaper sulla prevenzione della perdita dei dati.*
- *La gestione dei diritti sulle informazioni in Drive consente di disabilitare le funzioni di download, stampa e copia dei file dal menu di condivisione avanzata, nonché di impostare le date di scadenza per l'accesso ai file.*
- *La gestione dei dispositivi mobili consente di monitorare continuamente i sistemi e di essere avvisati in casi di attività sospette sui dispositivi.*

Per ulteriori informazioni, visita questa pagina web

Sicurezza dei prodotti: GCP

I clienti di GCP possono sfruttare le funzioni e le configurazioni del prodotto per proteggere ulteriormente i dati personali da possibili elaborazioni non autorizzate o illegali.

- *La verifica in due passaggi riduce sensibilmente il rischio di accessi non autorizzati mediante la richiesta di ulteriori prove dell'identità degli utenti che accedono. L'applicazione delle chiavi di sicurezza fornisce un livello aggiuntivo di protezione per gli account utente mediante la richiesta di una chiave fisica.*
- *Il sistema di gestione Google Cloud Identity and Access Management (Cloud IAM) consente di creare e gestire in modo dettagliato le autorizzazioni di accesso e modifica per le risorse di Google Cloud Platform.*
- *L'API Data Loss Prevention permette di identificare e monitorare l'elaborazione di categorie speciali di dati personali al fine di implementare controlli adeguati.*
- *Stackdriver Logging e Stackdriver Monitoring integrano sistemi di log, monitoraggio, avviso e rilevamento delle anomalie in Google Cloud Platform.*
- *Cloud Identity-Aware Proxy (Cloud IAP) controlla l'accesso alle applicazioni cloud eseguite su Google Cloud Platform.*
- *Cloud Security Scanner scansiona e rileva vulnerabilità comuni nelle applicazioni Google App Engine.*

Per ulteriori informazioni, visita questa pagina web

RESTITUZIONE ED ELIMINAZIONE DEI DATI

La funzionalità dei servizi G Suite o Google Cloud Platform consente agli amministratori di esportare i dati dei clienti in qualsiasi momento nel periodo di validità del contratto. Nei nostri termini di elaborazione dei dati abbiamo incluso una serie di impegni pluriennali per l'esportazione dei dati: continueremo a rispettarli anche dopo che il regolamento GDPR entrerà in vigore e a lavorare per potenziare l'efficacia della capacità di esportazione dei dati dei servizi G Suite e di ogni singolo servizio Google Cloud Platform (consulta la documentazione di Google Cloud Platform per ulteriori informazioni).

Mediante la funzionalità dei servizi G Suite o ***Google Cloud Platform*** *puoi anche eliminare i dati dei clienti in qualsiasi momento. Quando Google riceve una tua istruzione di eliminazione definitiva (come nel caso di un'email eliminata che non può più essere recuperata dal Cestino), eliminerà i dati pertinenti dei clienti da qualsiasi sistema entro un massimo di 180 giorni, a meno che non siano applicabili obblighi di conservazione.*

ASSISTENZA AL RESPONSABILE DEL TRATTAMENTO DEI DATI

Diritti dell'interessato

I responsabili del trattamento dei dati possono utilizzare le console di amministrazione di G Suite e Google Cloud Platform e la funzionalità dei relativi servizi per facilitare l'accesso ai dati nonché rettificare, limitare l'elaborazione o eliminare i dati che loro stessi o gli utenti immettono nei nostri sistemi. Questa funzionalità consente di rispettare l'obbligo a rispondere alle richieste degli interessati di esercitare i propri diritti delineati nel regolamento GDPR.

Team protezione dei dati

I clienti di G Suite e Google Cloud Platform hanno un team dedicato al quale è possibile inviare domande relative alla protezione dei dati.

Notifiche degli incidenti

G Suite e Google Cloud Platform garantiscono da diversi anni una serie di impegni contrattuali relativi alla notifica degli incidenti. Continueremo a informare prontamente i nostri clienti di eventuali incidenti relativi ai dati, secondo quanto delineato dai termini del nostro contratto attuale e dai termini aggiornati che si applicheranno a partire dal 25 maggio 2018, quando il regolamento GDPR entrerà in vigore.

TRASFERIMENTO DEI DATI INTERNAZIONALI

Il regolamento GDPR prevede vari meccanismi per facilitare il trasferimento dei dati personali al di fuori dell'UE. Questi meccanismi sono mirati a fornire un livello adeguato di protezione o ad assicurare l'implementazione di misure di salvaguardia appropriate al momento del trasferimento dei dati personali in un paese terzo.
Le misure di salvaguardia adeguate possono essere previste tramite clausole contrattuali tipo. È possibile garantire un livello adeguato di protezione mediante decisioni di adeguatezza come quelle che supportano lo scudo UE-USA per la privacy. Google si impegna contrattualmente a gestire un meccanismo che faciliti il trasferimento dei dati personali al di fuori dell'UE secondo quanto stabilito dalla direttiva per la protezione dei dati, nonché a garantire il proprio impegno a partire dal 25 maggio 2018 con l'entrata in vigore del regolamento GDPR. La certificazione di Google secondo gli scudi per la privacy UE-USA e Svizzera-USA include ***G Suite*** *e* ***Google Cloud Platform.*** *Gli enti europei per la protezione dei dati hanno inoltre confermato la conformità delle nostre clausole contrattuali tipo, dichiarando che i nostri impegni contrattuali per G Suite e Google Cloud Platform rispettano pienamente i requisiti previsti dalla direttiva per la protezione dei dati per quel che riguarda il trasferimento dei dati personali dall'UE al resto del mondo.*

STANDARD E CERTIFICAZIONI

I nostri clienti e gli enti regolatori si aspettano una verifica indipendente dei controlli relativi a sicurezza, privacy e conformità. A tale scopo, G Suite e Google Cloud Platform sono sottoposti regolarmente a numerose verifiche di terze parti indipendenti.

ISO 27001 (Gestione della sicurezza delle informazioni) - ISO 27001 è uno degli standard di sicurezza indipendenti più riconosciuti e accettati a livello internazionale. Google ha ottenuto la certificazione ISO 27001 per i sistemi, le applicazioni, le persone, la tecnologia, i processi e i data center che compongono la nostra infrastruttura comune condivisa e anche per i prodotti G Suite e Google Cloud Platform.

ISO 27017 (Sicurezza dei servizi cloud) - ISO 27017 è uno standard internazionale per i controlli della sicurezza delle informazioni basato su ISO/IEC 27002 e specifico per i servizi cloud. Google ha ottenuto la certificazione ISO 27017 per G Suite e Google Cloud Platform.

ISO 27018 (Privacy nella cloud) - ISO 27018 è uno standard internazionale per la protezione delle informazioni personali (PII, personally identifiable information) nei servizi cloud pubblici. Google ha ottenuto la certificazione ISO 27018 per G Suite e Google Cloud Platform.

SSAE16 / ISAE 3402 (SOC 2/3) - La struttura di audit SOC 2 (Service Organization Controls) e SOC 3 dell'American Institute of Certified Public Accountants (AICPA) definisce i princìpi fondamentali e i criteri relativi a sicurezza, disponibilità, integrità di elaborazione e riservatezza dei dati. Google ha ottenuto rapporti SOC 2 e SOC 3 per Google Cloud Platform e G Suite.

DOMANDE FREQUENTI

" COS'È IL REGOLAMENTO GDPR? "

Il General Data Protection Regulation è una nuova legislazione dell'UE sulla privacy che andrà a sostituire la Direttiva 95/46/CE sulla protezione dei dati del 24 ottobre 1995.

" QUANDO ENTRERÀ IN VIGORE IL REGOLAMENTO GDPR? "

Il regolamento GDPR sarà valido in tutti gli stati membro dell'Unione Europea a partire dal 25 maggio 2018.

" IL REGOLAMENTO GDPR PREVEDE L'ARCHIVIAZIONE DEI DATI PERSONALI NELL'UE? "

No. Come per la Direttiva 95/46/CE sulla protezione dei dati, il regolamento GDPR prevede determinate condizioni per il trasferimento dei dati personali al di fuori dell'UE. Tali condizioni possono essere rispettate attraverso meccanismi come le clausole contrattuali tipo.

" IL REGOLAMENTO GDPR DÀ DIRITTO AI CLIENTI DI SVOLGERE ATTIVITÀ DI AUDIT SU GOOGLE CLOUD? "

Secondo il regolamento GDPR, i diritti di audit devono essere concessi ai responsabili del trattamento dei dati nei contratti sottoscritti con i responsabili dell'elaborazione dei dati. Gli accordi sull'elaborazione dei dati aggiornati che applicheremo a partire dal 25 maggio 2018, quando il regolamento GDPR entrerà in vigore, includeranno pertanto diritti di audit a favore dei nostri clienti.

" QUAL È IL RUOLO DEGLI STANDARD ESTERNI ISO 27001, ISO 27017, ISO 27018 E DEI RAPPORTI SOC 2/3 PER QUEL CHE RIGUARDA LA CONFORMITÀ AL REGOLAMENTO GDPR? "

I clienti possono utilizzare le nostre certificazioni ISO di terze parti e i rapporti di audit SOC 2/3 per valutare meglio i rischi e determinare se vengono implementate misure tecniche e organizzative adeguate.

" QUALI ALTRE INFORMAZIONI HA FORNITO GOOGLE SUL REGOLAMENTO GDPR? "

Consulta **il sito web di Google per aziende e dati.**