



Informazioni sulla DPIA

Nome della PIA

Google Workspace Education

Nome autore

DPO Esempio Antonio

Nome validatore

DPO Esempio Antonio

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il Trattamento preso in considerazione è quello offerto dai servizi di Google inc, in relazione al passaggio di dati che avviene tra i Paesi Membri dell'Unione Europea e gli Stati Uniti.

Quali sono le responsabilità connesse al trattamento?

L'istituto scolastico è il Titolare del Trattamento e il Dirigente scolastico in quanto responsabile legale ha il compito di rispettare le norme vigenti del GDPR in materia di protezione dei dati e dei trasferimenti degli stessi verso i Paesi al di fuori dell'Unione Europea.

Google Inc. è Responsabile esterno al Trattamento dati essendo il provider dei servizi informatici utilizzati all'interno dell'Istituto scolastico, il servizio reso da Google deve presentare garanzie che mettano in atto misure tecniche e organizzative adeguate per rispettare i requisiti preposti del GDPR e allo stesso tempo deve garantire la tutela dei Diritti degli interessati.

Cosa afferma Google Inc. in merito al trattamento?

Google effettua il trattamento dei dati personali dei clienti dei servizi Google Cloud Platform, Google Workspace e Cloud Identity sulla base del Cloud Data Processing Addendum (CDPA). Il suddetto CDPA disciplina i trasferimenti internazionali di dati all'articolo 10, specificando che in caso il trasferimento avvenga verso un paese non coperto da una decisione di adeguatezza, allo stesso si applicano gli SCC, clausole contrattuali tipo, previste dall'articolo 46 GDPR (*<< if Google's address is not in an Adequate Country, the SCCs (Controller-to-Processor) and/or SCCs (Processor-to-Processor) will apply (according to whether Customer is a controller and/or processor) with respect to such Restricted European Transfers between Google and Customer.>>*

L'istituto scolastico utilizza i servizi resi gratuitamente dal Google inc del pacchetto Google Workspace Education, e su tali servizi si legge: *<< Google Workspace for Education può essere utilizzato in conformità con il GDPR. Il nostro Emendamento sul trattamento dei dati è progettato per soddisfare i requisiti di adeguatezza e sicurezza del GDPR; inoltre, la Commissione europea ha creato delle clausole contrattuali tipo per consentire in particolare il trasferimento dei dati personali dall'Europa. I clienti possono aderire all'Emendamento sul trattamento dei dati e alle clausole contrattuali tipo.>>*

Google inoltre mette a disposizione un link con domande utili reperibili al seguente URL:

https://edu.google.com/intl/ALL_it/why-google/privacy-security/frequently-asked-questions/



"Con l'Europa, investiamo nel vostro futuro"



<<Nel caso in cui i dati personali vengano trasferiti fuori dall'UE in paesi terzi non coperti da decisioni di adeguatezza, ci impegniamo a fronte dei nostri contratti per il trattamento dei dati a mantenere un meccanismo che faciliti questi trasferimenti secondo quanto stabilito dal GDPR.>> URL: <https://cloud.google.com/privacy/gdpr?hl=it>

Ci sono standard applicabili al trattamento?

Gli Standard definiti per il problema in esame fanno riferimento alla verifica sui singoli flussi di dati, in particolare che tali dati siano trasferiti secondo gli standard di adeguatezza come previsto dal GDPR. Il DPO deve verificare che i servizi ICT in uso siano conformi al GDPR attraverso i relativi accordi di servizio.

Versione di Google Workspace conforme e applicabile al trattamento?

L'Istituto scolastico utilizza, alla data del presente documento la versione Education di Google Workspace. Gli aggiornamenti di sicurezza sono rilasciati dalla piattaforma in modalità SaaS, quindi in modalità background, trasparente all'utente finale.

Definizione di Google Workspace applicata al trattamento?

Workspace (precedentemente noto come G Suite) è una suite integrata di applicazioni per la produttività e la collaborazione cloud-native e sicure. Tutti i piani forniscono un indirizzo personalizzato per la tua attività e includono strumenti di collaborazione (Gmail, Calendar, Meet, Chat, Drive, Documenti, Fogli, Presentazioni, Moduli, Sites, App Script, etc.); a seconda del piano scelto, è possibile utilizzare Google Cloud Search e AppSheet. Per la comunità scolastica, Google Workspace for Education (precedentemente noto come G Suite for Education) offre strumenti semplici, flessibili e sicuri per agevolare la collaborazione e la didattica, aiutando ad esempio gli insegnanti a risparmiare tempo con Classroom e Compiti per creare corsi, organizzare i lavori e condividere feedback.

Google Workspace è stata valutata dall'Agenzia Nazionale sulla Cybersicurezza?

I servizi di Google Workspace sono qualificati dall'Agenzia Nazionale sulla Cybersicurezza (ACN).

Google ha qualificato 70 servizi.

Workspace utilizza in particolar modo i primi 5, ma nelle applicazioni i restanti servizi possono essere utilizzati.

La qualificazione è proposta da **Google Cloud Italy S.r.l.** società iscritta al registro delle imprese in Italia.

Google Cloud Italy S.r.l. - <https://catalogocloud.acn.gov.it/service/785>

Google Workspace - <https://catalogocloud.acn.gov.it/service/690>

Google infrastruttura - <https://catalogocloud.acn.gov.it/service/271>

Google Cloud Storage - <https://catalogocloud.acn.gov.it/service/294>

Google Cloud Logging - <https://catalogocloud.acn.gov.it/service/273>

Google Cloud VMware Engine (GCVE) - <https://catalogocloud.acn.gov.it/service/3006>

reCAPTCHA Enterprise - <https://catalogocloud.acn.gov.it/service/3007>

Beyond Corp Enterprise - <https://catalogocloud.acn.gov.it/service/2321>

Network Connectivity Center (NCC) - <https://catalogocloud.acn.gov.it/service/3013>

Virtual Private Cloud (VPC) - <https://catalogocloud.acn.gov.it/service/3009>

Vertex AI - <https://catalogocloud.acn.gov.it/service/2320>

Artifact Registry - <https://catalogocloud.acn.gov.it/service/2514>

Cloud Data Loss Prevention (DLP) - <https://catalogocloud.acn.gov.it/service/2517>

Apigee X - <https://catalogocloud.acn.gov.it/service/2595>

Cloud CDN - <https://catalogocloud.acn.gov.it/service/2595>

Cloud Composer - <https://catalogocloud.acn.gov.it/service/2519>

Tel./ Fax. 081.7580785 - Sito web: www.palizzicasoria.edu.it - Email: naic8ev005@istruzione.it - Pec: naic8ev005@pec.istruzione.it



C.F. 93056840635 - Codice Univoco PA: UFE1J9



Cloud Hardware Security Module (HSM) - <https://catalogocloud.acn.gov.it/service/2521>
 Cloud Healthcare API - <https://catalogocloud.acn.gov.it/service/2520>
 Cloud External Key Manager (EKM) - <https://catalogocloud.acn.gov.it/service/2319>
 Cloud Data Fusion - <https://catalogocloud.acn.gov.it/service/2516>
 Cloud Data Catalog - <https://catalogocloud.acn.gov.it/service/2515>
 Anthos - <https://catalogocloud.acn.gov.it/service/2507>
 Traffic Director - <https://catalogocloud.acn.gov.it/service/2506>
 Cloud IDS - <https://catalogocloud.acn.gov.it/service/2505>
 Web Risk - <https://catalogocloud.acn.gov.it/service/2504>
 Cloud Error Reporting - <https://catalogocloud.acn.gov.it/service/797>
 Cloud Identity - <https://catalogocloud.acn.gov.it/service/689>
 Cloud Talent Solutions - <https://catalogocloud.acn.gov.it/service/388>
 API Video Intelligence - <https://catalogocloud.acn.gov.it/service/376>
 Cloud Functions - <https://catalogocloud.acn.gov.it/service/371>
 API Cloud Speech-to-Text - <https://catalogocloud.acn.gov.it/service/370>
 API Cloud Text-to-Speech - <https://catalogocloud.acn.gov.it/service/360>
 Google Cloud Interconnect - <https://catalogocloud.acn.gov.it/service/357>
 Cloud Armor - <https://catalogocloud.acn.gov.it/service/783>
 Cloud Container Registry - <https://catalogocloud.acn.gov.it/service/784>
 Cloud Trace - <https://catalogocloud.acn.gov.it/service/794>
 Cloud Build - <https://catalogocloud.acn.gov.it/service/786>
 Cloud Source Repositories - <https://catalogocloud.acn.gov.it/service/788>
 Cloud Firestore - <https://catalogocloud.acn.gov.it/service/374>
 Google Cloud Key Management Service - <https://catalogocloud.acn.gov.it/service/367>
 Cloud DNS - <https://catalogocloud.acn.gov.it/service/358>
 Google Cloud IoT Core - <https://catalogocloud.acn.gov.it/service/362>
 Cloud Spanner - <https://catalogocloud.acn.gov.it/service/372>
 Cloud Run - <https://catalogocloud.acn.gov.it/service/369>
 Cloud NAT (Network Address Translation) - <https://catalogocloud.acn.gov.it/service/366>
 App Engine - <https://catalogocloud.acn.gov.it/service/361>
 Dialogflow - <https://catalogocloud.acn.gov.it/service/359>
 Cloud VPN - <https://catalogocloud.acn.gov.it/service/356>
 Cloud Datastore - <https://catalogocloud.acn.gov.it/service/373>
 Cloud Natural Language - <https://catalogocloud.acn.gov.it/service/378>
 Cloud AutoML Vision - <https://catalogocloud.acn.gov.it/service/389>
 Cloud Memorystore - <https://catalogocloud.acn.gov.it/service/368>
 Cloud Vision API - <https://catalogocloud.acn.gov.it/service/377>
 Cloud Firebase - <https://catalogocloud.acn.gov.it/service/375>
 Security Command Center - <https://catalogocloud.acn.gov.it/service/1828>
 AlloyDB - <https://catalogocloud.acn.gov.it/service/1829>
 Bare Metal Solution (BMS) - <https://catalogocloud.acn.gov.it/service/1833>
 Cloud SQL - <https://catalogocloud.acn.gov.it/service/284>
 Google Kubernetes Engine - <https://catalogocloud.acn.gov.it/service/283>
 Cloud Dataproc - <https://catalogocloud.acn.gov.it/service/299>
 Cloud Dataflow - <https://catalogocloud.acn.gov.it/service/298>
 Cloud Pub/Sub - <https://catalogocloud.acn.gov.it/service/300>
 Google Translation API - <https://catalogocloud.acn.gov.it/service/272>
 Google Cloud Bigtable - <https://catalogocloud.acn.gov.it/service/275>
 Google BigQuery - <https://catalogocloud.acn.gov.it/service/297>

Cloud Monitoring - <https://catalogocloud.acn.gov.it/service/274>

Google Compute Engine - <https://catalogocloud.acn.gov.it/service/293>

Google Cloud Load Balancing - <https://catalogocloud.acn.gov.it/service/296>

Apigee - <https://catalogocloud.acn.gov.it/service/1251>

Stackdriver Debugger - <https://catalogocloud.acn.gov.it/service/796>

Valutazione: Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati oggetto di trasferimento transfrontaliero sono l'indirizzo IP del dispositivo dell'utente e le informazioni relative al browser, al sistema operativo, alla risoluzione dello schermo, alla lingua selezionata e alla data e ora della visita al sito web, questi dati raccolti e trasferiti sono conservati per un tempo di 18 mesi. I soggetti che possono accedere a questi dati sono i dipendenti di Google in., le società consociate o le società che agiscono per conto di Google inc., sono tutti vincolati ai termini di riservatezza e opportunamente incaricati al trattamento ai sensi dell'art. 28,c del Regolamento Europeo 679/2016 (data verifica DPO, 31/03/2023)

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Il ciclo di vita passa attraverso una serie di fasi: si va dalla raccolta di dati personali, alla manipolazione durante la fase di espletamento e dell'utilizzo dei servizi offerti, alla conservazione e all'archiviazione, fino alla distruzione degli stessi dopo 18 mesi.

Quali sono le risorse di supporto ai dati?

Le risorse che ospitano le informazioni sono le varie strumentazioni informatiche utilizzate che possono essere tablet, pc, smartphone, che sono basati su diversi sistemi operativi che permettono la fruizione dei servizi offerti da Google.

Valutazione: Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Si ritiene che il Trattamento sia svolto nell'interesse pubblico ovvero per poter svolgere l'attività di formazione e istruzione nei confronti degli studenti, diritto sancito a livello Costituzionale ex art.34.
Inoltre il Trattamento su strumenti CLOUD è altamente consigliato perché più sicuro rispetto all'uso tradizionale.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Le basi legali che rendono lecito il trattamento sono:

- La Costituzione nell'art.34 sancisce il diritto all'istruzione.
- I contratti stipulati tra il Titolare del trattamento (le istituzioni scolastiche) e i Responsabili del trattamento (Google),



ovvero rispettivamente *Cloud Data Processing Addendum CDPA* e *Data Processing Agreement DPA*; all'interno di questi sono presenti clausole che autorizzano la legittimità del Trattamento posto in essere.

Google Workspace è un servizio SaaS qualificato dall'Agenzia Italiana per la Cybersicurezza Nazionale (ACN), la scheda di servizio qualificato è disponibile al seguente URL: <https://catalogocloud.acn.gov.it/service/690>

Nella scheda del servizio qualificato si legge:

Workspace (precedentemente noto come G Suite) è una suite integrata di applicazioni per la produttività e la collaborazione cloud-native e sicure. Tutti i piani forniscono un indirizzo personalizzato per la tua attività e includono strumenti di collaborazione (Gmail, Calendar, Meet, Chat, Drive, Documenti, Fogli, Presentazioni, Moduli, Sites, App Script, etc.); a seconda del piano scelto, è possibile utilizzare Google Cloud Search e AppSheet. Per la comunità scolastica, Google Workspace for Education (precedentemente noto come G Suite for Education) offre strumenti semplici, flessibili e sicuri per agevolare la collaborazione e la didattica, aiutando ad esempio gli insegnanti a risparmiare tempo con Classroom e Compiti per creare corsi, organizzare i lavori e condividere feedback.

Valutazione: Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati raccolti sono necessari al trattamento in quanto si parla di dati che permettono la connessione e l'utilizzo delle tecnologie e dei servizi che rendono l'Istruzione digitalizzata, in un Mondo che va sempre più verso questa direzione.

Google nel rispetto dei principi di minimizzazione e conservazione del dato digitale opera la cifratura AES del dato archiviato sui servizi. Gli standard e le certificazioni di Google sono numerosissime quelle necessarie al trattamento sono le seguenti: rif.: - <https://workspace.google.com/learn-more/security/security-whitepaper/page-8.html#eu-data-protection> - <https://cloud.google.com/security/compliance>

Google è in possesso della certificazione ISO/IEC 27001 estesa con i controlli degli standard ISO/IEC 27017 e ISO/IEC 27018 disponibile al seguente link https://catalogocloud.acn.gov.it/serve/690/docs/ec76fc8aee48b311160bf9c9b853cfe89ed2a7801e0be82ad6a0922536a2d3cc/MAY_2021_Google_Workspace_ISO.pdf

Valutazione: Accettabile

I dati sono esatti e aggiornati?

Le misure previste per garantire la qualità dei dati sono quelle previste all'interno dei contratti stipulati, CDPA e DPA.

CDPA: <https://cloud.google.com/terms/data-processing-addendum>

DPA: https://www.google.com/analytics/terms/dpa/dataprocessingamendment_20200816.html

Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?

Tutti i dati conservati da Google nei servizi Cloud storage sono resi anonimi, minimizzati e cifrati. Inoltre sono evirati parzialmente dell'indirizzo IP (dopo 9 mesi) e delle informazioni sui cookie (dopo 18 mesi).
Dopo 18 mesi sono cancellati come previsto dalla normativa europea.

Valutazione: Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati sono informati tramite apposite informative connesse al consenso e qualora i dati dovessero essere utilizzati per uno scopo non contemplato nelle norme riferite alla privacy si richiede un ulteriore consenso. Nella sezione Controllo privacy si ha l'opportunità di esaminare e modificare tutte le informazioni riguardanti la privacy. Ogni utente è libero di personalizzare il proprio account in termini di privacy, l'amministratore di sistema, opportunamente designato, applica periodicamente controlli e aggiornamenti globali alla piattaforma, tali aggiornamenti di sicurezza si applicano verticalmente a tutti gli utenti.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Il Consenso si ottiene attraverso l'accettazione delle varie clausole ponendo una spunta in fase di registrazione. Per gli studenti il consenso è richiesto in fase di rilascio dell'account. E' espresso dai tutori legali per gli studenti minorenni.

Valutazione: Accettabile

Dove sono geolocalizzati i server di Google in Europa?

I server di Google in Europa sono diversi e sono in:

- Dublino, Irlanda - <https://www.google.com/intl/it/about/datacenters/locations/dublin/>
- Hamina, Finlandia - <https://www.google.com/intl/it/about/datacenters/locations/hamina/>
- Saint-Ghislain, Belgio - <https://www.google.com/intl/it/about/datacenters/locations/st-ghislain/>
- Fredericia, Danimarca - <https://www.google.com/intl/it/about/datacenters/locations/fredericia/>
- Middenmeer, Paesi Bassi - <https://www.google.com/intl/it/about/datacenters/locations/middenmeer/>

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Gli interessati possono rivolgersi direttamente all'amministratore designato dall'Istituto per l'esercizio dei loro diritti.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?



Gli interessati possono rivolgersi direttamente all'amministratore designato dall'Istituto per l'esercizio dei loro diritti.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Gli interessati possono rivolgersi direttamente all'amministratore designato dall'Istituto per l'esercizio dei loro diritti.

Valutazione: Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

I Responsabili del trattamento sono legati al Titolare da un contratto che viene accettato e all'interno dello stesso sono descritti gli ambiti di responsabilità e gli obblighi specifici con relative incombenze.

Valutazione: Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

In caso di trasferimento verso Paesi Esteri secondo la nota Ministeriale n. 0000706 del 20.03.2023, i dati possono essere trasferiti ai sensi dell'art. 45 del GDPR solo se si forniscono garanzie adeguate e a condizione che gli interessati dispongano dei diritti azionabili e di mezzi di ricorso effettivi (misure adeguate ex art.46 GDPR); quindi alla stipula contrattuale il Titolare del trattamento e il Responsabile del trattamento adeguano i contratti rispetto alla normativa prevista dal GDPR in modo tale da offrire tutela anche per il trasferimento dati verso Paesi fuori dall'Unione Europea.

Il regolamento generale sulla protezione dei dati dell'Unione europea (UE) regola il trasferimento dei dati personali dei clienti UE verso paesi al di fuori dell'Area Economica Europea (AEE) che include tutti i paesi dell'Unione Europea, Islanda, Liechtenstein e Norvegia. A livello pratico, la conformità alle leggi sulla protezione dei dati dell'UE significa anche che i clienti hanno bisogno di meno approvazioni da parte delle singole autorità per trasferire i dati personali al di fuori dell'UE, poiché la maggior parte degli Stati membri dell'UE non richiede un'autorizzazione aggiuntiva se il trasferimento è basato su un accordo conforme alle clausole modello.

Google informa l'utente

Gestiamo server in tutto il mondo e le tue informazioni potrebbero essere elaborate su server situati al di fuori del paese in cui vivi. Le leggi in materia di protezione dei dati personali variano da paese a paese e alcune prevedono più protezione di altre. Indipendentemente da dove sono elaborate le tue informazioni, noi applichiamo le stesse tutele descritte nelle [Norme sulla privacy](#). Inoltre, rispettiamo alcune normative vigenti relative al trasferimento dei dati, tra cui le normative descritte di seguito.

La Commissione europea ha stabilito che alcuni paesi esterni allo Spazio economico europeo (SEE) sono tenuti a proteggere i dati personali in maniera adeguata, il che significa che i dati possono essere trasferiti dall'Unione europea (UE), dalla Norvegia, dal Liechtenstein e dall'Islanda al paese terzo senza che siano necessarie ulteriori salvaguardie. Il Regno Unito e la Svizzera hanno approvato decisioni di adeguatezza simili. In alcuni casi ci basiamo sulle seguenti

decisioni di adeguatezza: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Le clausole contrattuali tipo (SCC) sono impegni scritti tra le parti che possono essere usati come base per i trasferimenti di dati dall'Unione europea a paesi terzi fornendo le adeguate salvaguardie per la protezione dei dati. Le SCC sono state approvate dalla Commissione europea e non possono essere modificate dalle parti che le utilizzano (puoi controllare le SCC adottate dalla Commissione europea [qui](#), [qui](#) e [qui](#)). Queste clausole sono state approvate anche per i trasferimenti di dati a paesi diversi dal Regno Unito e dalla Svizzera. Ove richiesto, ci basiamo sulle SCC per i nostri trasferimenti di dati. Se vuoi una copia delle SCC, [contattaci](#).

Google incorpora le SCC anche nei contratti stipulati con tutti i clienti dei suoi servizi per aziende, tra cui [Google Workspace](#), [Google Cloud Platform](#), [Google Ads](#) e altri [prodotti pubblicitari e di misurazione](#). Puoi trovare ulteriori informazioni all'indirizzo privacy.google.com/businesses.

Dal 16 luglio 2020 Google non basa più sull'EU-U.S. Privacy Shield (scudo UE-USA per la privacy) per trasferire dati dallo Spazio economico europeo e dal Regno Unito negli Stati Uniti.

Alla data del presente documento nessun provvedimento del Garante Italiano sulla Privacy è prodotto contro lo strumento Google Workspace Education

Valutazione: Accettabile

Rischi

Misure esistenti o pianificate

Crittografia

I dati sono trattati tramite l'utilizzo di meccanismi di conservazione e comunicazioni cifrati, ai fini di garantire la minimizzazione del rischio di accesso agli stessi.

L'amministratore di sistema opportunamente designato dall'Istituto scolastico è in grado di accedere a tali prospetti, non può accedere alle informazioni, ma può verificare che i dati siano integri e opportunamente protetti.

Valutazione: Accettabile

Anonimizzazione

Gli indirizzi IP (dato particolare oggetto di trasferimento) sono in anonimizzati così da garantire il diritto alla riservatezza e il rispetto del principio di minimizzazione dei dati.

Valutazione: Accettabile

Accesso illegittimo ai dati - **RISCHIO**

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Diffusione di dati personali di minori, concernenti le attrezzature utilizzate dagli stessi (device) per l'utilizzo dei servizi offerti dai responsabili del Trattamento.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Negazione del diritto all'oblio, rischio arginabile in quanto è possibile presentare ricorso all'autorità di garanzia europea e statunitense.

Quali sono le fonti di rischio?

La fonte di rischio risiede nello stesso trasferimento dati, i dati trasferiti sono dati di tipo particolare. rischio arginabile in quanto l'impatto sulla sfera privata dell'interessato è minimo. Le informazioni riguardano i device utilizzati e pertanto il dato oggetto di rischio è minimo.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Anonimizzazione, VPN, Firewall.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile, Il rischio è da ritenere trascurabile in quanto i dati oggetto di trasferimento nei Paesi al di fuori dell'Unione Europea sono anonimizzati inoltre i dati se pur di categoria particolare (indirizzo IP, ecc..) non hanno un impatto rilevante nei confronti della sfera giuridica privata degli interessati.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, in quanto la tutela offerta dagli stessi contratti stipulati permette di limitare qualsiasi violazione ad alto impatto. La diffusione involontaria dei dati causerebbe un danno all'immagine di Google nel contesto globale, la stessa società è impegnata nella sicurezza in modo preponderante.

Valutazione: Accettabile

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Diffusione dei dati personali di minori, concernenti le attrezzature utilizzate dagli stessi per l'utilizzo di servizi offerti dai Responsabili del Trattamento

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Negazione del diritto all'oblio, rischio arginabile in quanto è possibile presentare ricorso all'autorità di garanzia europea e statunitense.

Quali sono le fonti di rischio?

La fonte di rischio risiede nello stesso trasferimento dati, i dati trasferiti sono dati di tipo particolare. rischio arginabile in quanto l'impatto sulla sfera privata dell'interessato è minimo. Le informazioni riguardano i device utilizzati e pertanto il dato oggetto di rischio è minimo.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Anonimizzazione, VPN, Firewall.

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile, Il rischio è da ritenere trascurabile in quanto i dati oggetto di trasferimento nei Paesi al di fuori dell'Unione Europea sono anonimizzati inoltre i dati se pur di categoria particolare (indirizzo IP, ecc..) non hanno un impatto rilevante nei confronti della sfera giuridica privata degli interessati.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, in quanto la tutela offerta dagli stessi contratti stipulati permette di limitare qualsiasi violazione ad alto impatto. La diffusione involontaria dei dati causerebbe un danno all'immagine di Google nel contesto globale, la stessa società è impegnata nella sicurezza in modo preponderante.

Valutazione: Accettabile

Perdita di dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Diffusione dei dati personali di minori, concernenti le attrezzature utilizzate dagli stessi per l'utilizzo di servizi offerti dai Responsabili del Trattamento

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Negazione del diritto all'oblio, rischio arginabile in quanto è possibile presentare ricorso all'autorità di garanzia europea e statunitense.

Quali sono le fonti di rischio?

La fonte di rischio risiede nello stesso trasferimento dati, i dati trasferiti sono dati di tipo particolare. rischio arginabile in quanto l'impatto sulla sfera privata dell'interessato è minimo. Le informazioni riguardano i device utilizzati e pertanto il dato oggetto di rischio è minimo.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Anonimizzazione, VPN, Firewall.

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile, Il rischio è da ritenere trascurabile in quanto i dati oggetto di trasferimento nei Paesi al di fuori dell'Unione Europea sono anonimizzati inoltre i dati se pur di categoria particolare (indirizzo IP, ecc..) non hanno un impatto rilevante nei confronti della sfera giuridica privata degli interessati.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, in quanto la tutela offerta dagli stessi contratti stipulati permette di limitare qualsiasi violazione ad alto impatto. La diffusione involontaria dei dati causerebbe un danno all'immagine di Google nel contesto globale, la stessa società è impegnata nella sicurezza in modo preponderante.

Valutazione: Accettabile

Panoramica dei rischi

Impatti potenziali

Diffusione dei dati persona

Minaccia

Negazione del diritto all'o..

Fonti

La fonte di rischio può ess..

Misure

Crittografia

Anonimizzazione

Accesso illegittimo ai dati

Gravità : Trascurabile

Probabilità : Trascurabile

Modifiche indesiderate dei dati

Gravità : Trascurabile

Probabilità : Trascurabile

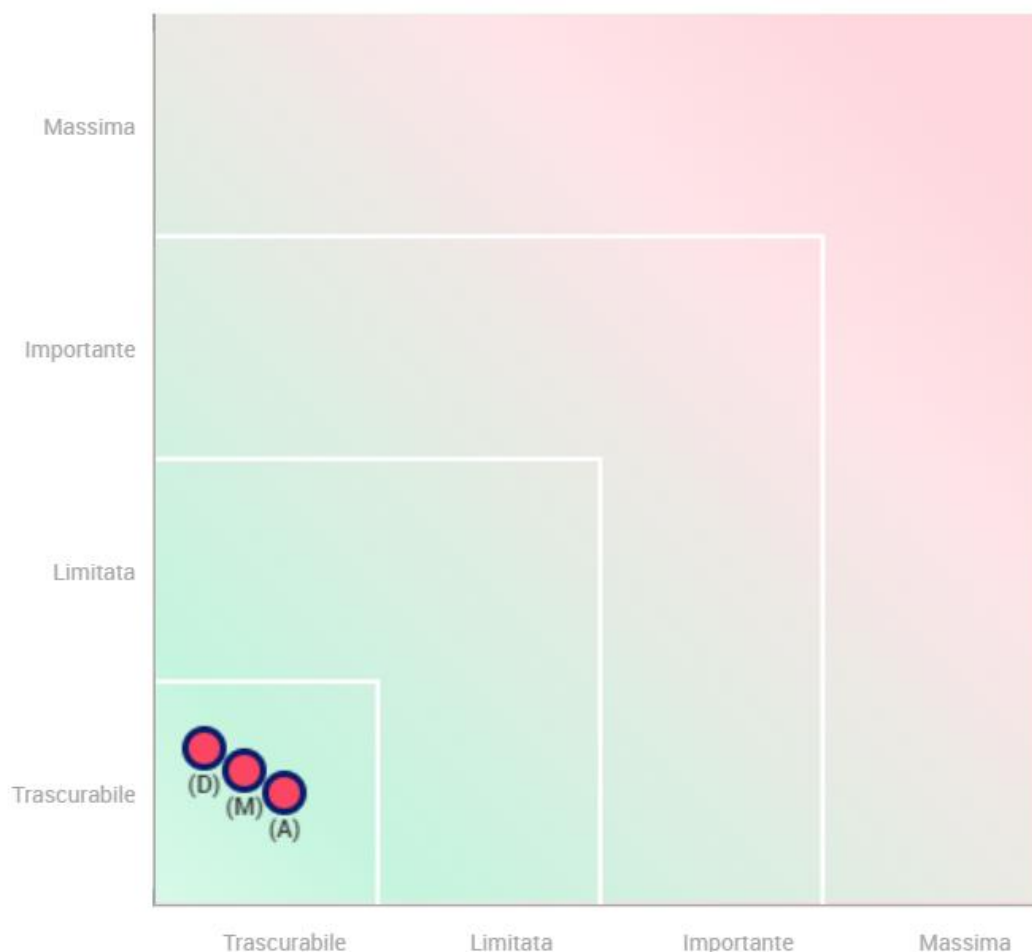
Perdita di dati

Gravità : Trascurabile

Probabilità : Trascurabile

Mappa dei rischi

Gravità del rischio



- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

Probabilità del rischio

22/03/23

Piano d'azione

Panoramica

Principi fondamentali

Finalità	
Basi legali	
Adeguatezza dei dati	
Esattezza dei dati	
Periodo di conservazione	
Informativa	
Raccolta del consenso	
Diritto di accesso e diritto alla portabilità dei dati	
Diritto di rettifica e diritto di cancellazione	
Diritto di limitazione e diritto di opposizione	
Responsabili del trattamento	
Trasferimenti di dati	

Misure esistenti o pianificate

	Crittografia
	Anonimizzazione

Rischi

	Accesso illegittimo ai dati
	Modifiche indesiderate dei dati
	Perdita di dati

Misure Migliorabili

Misure Accettabili

Il DPO

Esempio Antonio

