- **Oggetto:** POSTA CERTIFICATA: [RIF PA08.istsc_anic834008] Segnalazione di trasferimenti sistematici di dati personali verso Google e conseguente invito a risolvere la violazione del Regolamento Europeo 2016/679 (GDPR)
- **Data ricezione email:** 01/03/2023 02:44
- **Mittenti:** comunicazioni@pec.monitora-pa.it - Gest. doc. - Email: comunicazioni@pec.monitora-pa.it
- **Indirizzi nel campo email 'A':** ISTITUTO COMPRENSIVO - CORINALDO <anic834008@pec.istruzione.it>
- **Indirizzi nel campo email 'CC':**
- **Indirizzo nel campo 'Rispondi A':** <comunicazioni@pec.monitora-pa.it>

Allegati

File originale	Bacheca digitale?	Far firmare a	Firmato da	File firmato	File segnato
daticert.xml	SI			NO	NO
postacert.eml	SI			NO	NO

Testo email

Messaggio di posta certificata

Il giorno 01/03/2023 alle ore 02:44:12 (+0100) il messaggio
"[RIF PA08.istsc_anic834008] Segnalazione di trasferimenti sistematici di dati personali verso Google e conseguente invito a risolvere la violazione del Regolamento Europeo 2016/679 (GDPR)"
è stato inviato da "comunicazioni@pec.monitora-pa.it"
indirizzato a:

- anic834008@pec.istruzione.it

Il messaggio originale è incluso in allegato.
Identificativo messaggio: opec2115.20230301024413.16008.19.1.81@certmail.irideos.it

All'attenzione di:

- ISTITUTO COMPRENSIVO - CORINALDO, in qualità di
soggetto titolare del trattamento ai sensi dell'art. 4 par. 1 n. 7 - GDPR.

Il sottoscritto Fabio Pietrosanti, nato a Latina il 31/08/1980
(codice fiscale: PTRFBA80M31E472W), scrive nell'ambito
nel progetto Monitora PA (https://monitora-pa.it) e con il
sostegno dei cittadini che vi collaborano e delle associazioni
elencate in calce, eleggendo ai fini del presente atto
a domicilio digitale l'indirizzo di posta elettronica
certificata comunicazioni@pec.monitora-pa.it, e a domicilio
fisico via Aretusa 34, a Milano c/o Hermes Center.

1. Tramite l'esecuzione dell'osservatorio di Monitora PA,
in data 2023-02-28 18:45:11.520270, ho rilevato che il vostro Ente
ISTITUTO COMPRENSIVO - CORINALDO
utilizza per la posta elettronica ordinaria
(PEO) i servizi forniti da Google LLC.

2. L'adozione dei servizi di posta elettronica forniti da Google determina trasferimenti sistematici di dati personali degli utenti e dei loro corrispondenti, non attualmente conformi, in assenza di efficaci misure tecniche supplementari, alle disposizioni del GDPR in ordine al trasferimento transfrontaliero di dati personali, fra cui, a titolo esemplificativo ma non esaustivo:

- indirizzo IP
- indirizzo email
- Mail User Agent
- sistema operativo
- relazioni inter-personali
- dati personali descrittivi deducibili dall'incrocio dei dati precedenti, dall'oggetto e dai contenuti dei messaggi trasmessi

3. Tale circostanza può essere verificata facilmente traminte l'analisi dei i record MX sul DNS del vostro dominio email iccorinaldo.edu.it

- 10 aspmx.l.google.com.
- 20 alt1.aspmx.l.google.com.
- 20 alt2.aspmx.l.google.com.
- 30 alt3.aspmx.l.google.com.
- 30 alt4.aspmx.l.google.com.

Le informazioni inviate durante tali trasferimenti, che coinvolgono ovviamente anche persone che decidano di corrispondere con un Vostro indirizzo di PEO, sono più che sufficienti ad identificare mittenti e destinatari, tracciarne le comunicazioni e ad arricchirne i profili cognitivo-comportamentali.

4. Come ben noto anche a seguito della sentenza Schrems II della Corte di Giustizia dell'Unione Europea, l'uso dei servizi sopra elencati non è attualmente conforme, in assenza di misure tecniche supplementari efficaci che non ci risultano indicate sul vostro sito, alle disposizioni del GDPR in ordine al trasferimento transfrontaliero dei dati personali verso gli Stati Uniti o altri Paesi la cui legislazione non fornisca ai cittadini europei una protezione equivalente a quella garantita nell'Unione.

5. Anche l'EDPB, con le Raccomandazioni 01/2020, ha precisato che si possono trasferire dati personali in tali Paesi utilizzando altre basi legali (come le clausole contrattuali tipo di protezione dei dati) ma solo adottando efficaci misure tecniche supplementari (per esempio la cifratura dei dati personali con chiavi indisponibili ai riceventi) di modo che non sia possibile utilizzare i dati personali in violazione dei diritti fondamentali dei cittadini europei al di fuori dell’UE.

6. Il Garante per la protezione dei dati personali della Danimarca, in un caso riguardante l'uso dei Chromebook e di Google Workspace nelle scuole del comune di Helsingør, ha emesso in data 14 luglio 2022 un provvedimento nel quale ha evidenziato gravi violazioni e ha vietato il trasferimento dei dati a paesi terzi e l'uso di Google Workspace. [^1]

7. Durante l'esame tecnico organizzativo sulla piattaforma Microsoft Office 365, compreso Microsoft Teams, nella configurazione del progetto pilota del Ministero dell'Istruzione del Baden - Württemberg, il locale Garante per la protezione dei dati personali ha riscontrato alcune gravi carenze e numerose criticità nell'uso a fini didattici di tali piattaforme. [^2]

8. La Conferenza sulla protezione dei dati (Datenschutzkonferenz, DSK), l'organismo delle autorità tedesche indipendenti di controllo della protezione dei dati a livello federale e statale, il 7/12/2022 ha pubblicato la Relazione finale del gruppo di lavoro DSK "Servizi online di Microsoft" nella quale si leggono le seguenti Conclusioni: "L'utilizzo di Microsoft 365... ...richiede istruzioni obbligatorie da parte del responsabile del trattamento sul trasferimento dei dati personali a paesi terzi, in particolare gli Stati Uniti e tutti gli altri paesi in cui Microsoft o i suoi subprocessori sono attivi. In ogni caso, il trasferimento di dati verso gli Stati Uniti non può essere impedito nemmeno tecnicamente. In particolare, la legge statunitense sulla sicurezza nazionale sotto forma di FISA 702 può mettere in discussione l'adempimento degli obblighi previsti dalle clausole contrattuali standard. Pertanto, sarebbe necessario adottare misure di protezione supplementari per rendere impossibile o inefficace qualsiasi accesso da parte delle autorità statunitensi e anche da parte di Microsoft e dei suoi dipendenti, al fine di impedire a Microsoft di soddisfare le richieste di consegna ai sensi del FISA 702. Tuttavia, l'uso dei servizi Microsoft 365 come servizi cloud classici richiede a Microsoft di accedere a dati in chiaro in molti casi d'uso... ...Le misure fornite da Microsoft sono insufficienti..." [^3]

9. Nel documento "2022 Azione esecutiva coordinata - Utilizzo di servizi basati su cloud da parte del settore pubblico" adottato come raccomandazione il 17 gennaio 2023 l'EDPB ribadisce che: "..l'utilizzo da parte di un ente pubblico del software fornito dal fornitore di servizi cloud può comportare trasferimenti verso molte destinazioni che non garantiscono un livello di protezione sostanzialmente equivalente a quello dell'UE, compresi gli Stati Uniti d'America (USA).
In questi casi, l'ente pubblico - che agisce in qualità di titolare del trattamento - deve valutare attentamente i trasferimenti che possono essere effettuati per suo conto dal fornitore di servizi cloud, ad esempio identificando le categorie di dati personali trasferiti, le finalità, i soggetti a cui i dati possono essere trasferiti e il paese terzo coinvolto.
La valutazione dei trasferimenti internazionali di dati personali in atto dovrebbe essere effettuata prima di impegnarsi con il fornitore di servizi cloud. Gli enti pubblici devono fornire istruzioni all'incaricato del trattamento per individuare e utilizzare uno strumento di trasferimento adeguato e, se necessario, per individuare e attuare misure supplementari appropriate che garantiscano che le garanzie contenute nello strumento di trasferimento prescelto possano essere rispettate dall'importatore, in modo da assicurare che il livello di protezione offerto dal GDPR non sia compromesso quando i dati sono trasferiti a un paese terzo. [...]
Emerge dall'analisi effettuata dalle Autorità che il solo uso di un Cloud Service Provider che sia parte di un gruppo multinazionale soggetto alla normativa di paesi terzi, può risultare nell'applicazione di tale normativa anche a dati salvati nel EEA. Eventuali richieste verrebbero inviate direttamente al CSP presente nel EEA e riguarderebbero dati presenti nel EEA e non dati già oggetto di trasferimenti." [^4]

10. Human Rights Watch quest'anno ha pubblicato un rapporto sulle violazioni della privacy di studenti, genitori ed insegnanti da parte delle piattaforme educative adottate durante la pandemia. [^5]

11. Infine L'Autorità Garante per la Protezione dei dati Personali italiana con Provvedimento del 9 giugno 2022 [docweb n. 9782890] , pubblicato il 23 giugno 2022, ha richiamato "all'attenzione di tutti i gestori italiani di siti web, pubblici e privati, l'illiceità dei trasferimenti effettuati verso gli Stati Uniti attraverso GA" e invitato "tutti i titolari del trattamento a verificare la conformità delle modalità di utilizzo di cookie e altri strumenti di tracciamento utilizzati sui propri siti web, con particolare attenzione a Google Analytics e ad altri servizi analoghi, con la normativa in materia di protezione dei dati personali".

12. Il servizio di posta elettronica GMail ed eventualmente ogni altro servizio che determini analoghi trasferimenti, come Google Drive, Google Documents o Google Workspace, per la loro modalità di funzionamento, costituiscono di fatto strumenti di tracciamento e profilazione degli utenti, contrari ai principi ed alle norme del GDPR.

13. Inoltre non è mai possibile escludere che l'utilizzo di detti servizi comporti il trasferimento di dati personali appartenenti alle speciali categorie protette dall'articolo 9 del GDPR.
Ad esempio una scuola potrebbe inavvertitamente cedere a Google LLC informazioni sulla religione di uno studente attraverso dati sulla sua partecipazione agli insegnamenti facoltativi della Religione Cattolica; un ospedale potrebbe informare Google LLC sulle patologie che affliggono un determinato paziente permettendo ai medici alla propria dipendenza di comunicare via email tali dati o più in generale una qualsiasi PA potrebbe rendere disponibili i dati sanitari di un proprio dipendente a Google, che li processerebbe per le proprie finalità. [^6]

14. Ritengo quindi che i trasferimenti di dati personali sopra indicati non siano conformi al disposto normativo vigente - in ragione del trasferimento trasfrontaliero di dati personali e in assenza di una condizione legittimante ai sensi degli artt. 44 e ss. GDPR - e che quindi espongano a rischi ingiustificati tutti gli utenti dei servizi ed i loro corrispondenti.

15. Pertanto invito l'Ente in indirizzo a voler provvedere alla rimozione dei servizi sopra indicati, entro il termine di 60 giorni dalla ricezione della presente.

16. In alternativa e negli stessi termini, invito il vostro Ente ad adottare misure tecniche supplementari efficaci a protezione dei dati personali degli interessati coinvolti nel funzionamento del Vostro sistema di PEO tali che nessun dato (o insieme di dati), raggiungendo i server di Google, possa permettere di identificare con probabilità non trascurabile, tracciare le comunicazioni e ad arricchirne i profili cognitivo-comportamentali di un qualsiasi cittadino italiano o europeo.

17. In difetto di ottemperanza da parte Vostra, nel termine sopra indicato, agli obblighi di legge in materia di trattamento dei dati personali, mi vedrò costretto a rivolgermi al Garante per la protezione

dei dati personali, ai sensi e per gli effetti degli artt. 141 e seguenti del Codice in materia di protezione dei dati personali (DECRETO LEGISLATIVO 30 giugno 2003, n.196 e successive modifiche e integrazioni) per una valutazione della Vostra condotta anche ai fini dell'emanazione di eventuali provvedimenti di cui all'art. 58 del GDPR.

Rimango a disposizione per ulteriori chiarimenti.

Con osservanza.

Distinti saluti

Milano, 01/03/2023

Fabio Pietrosanti
Co-fondatore del progetto Monitora PA
https://monitora-pa.it

Con il sostegno di:

- Hermes Center, Associazione con sede in Via Aterusa n. 34, 20129 Milano, in persona del legale rappresentante p.t Fabio Pietrosanti C.F. 97621810155 https://www.hermescenter.org/
- LinuxTrent, Associazione con sede in Via Marconi n. 105, 38057 Pergine Valsugana, in persona del legale rappresentante p.t Roberto Resoli C.F. 96100790227 https://www.linuxtrent.it/
- Open Genova, Associazione con sede in Piazza Matteotti n. 5 c/o Mentelocale.it, 16123 Genova, in persona del legale rappresentante p.t Pietro Biase C.F. 95165570102 https://associazione.opengenova.org/
- AsCII, Associazione con sede in Via del Mare n.108, 80016 Marano di Napoli, in persona del legale rappresentante p.t Avvocato Marco Andreoli C.F. 94200750639 https://www.ascii.it/
- AsSoLi, Associazione con sede in Via San Quintino n. 32, 10121 Torino, in persona del legale rappresentante p.t Angelo Raffaele Meo C.F. 94082140487 https://www.softwarelibero.it/

---

[^1]: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/datatilsynet-nedlaegger-behandlingsforbud-i-chromebook-sag-
[^2]: https://www.baden-wuerttemberg.datenschutz.de/ms-365-schulen-hinweise-weiteres-vorgehen/
[^3]: https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf
[^4]: https://edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf
[^5]: https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments
[^6]: è importante notare come tali finalità includano esplicitamente
- "migliorare i nostri servizi"

- "sviluppare nuovi prodotti e funzionalità"
- "mostrare pubblicità"
- "effettuare ricerche"
- rispondere "a una richiesta esecutiva del governo"

https://policies.google.com/privacy?hl=it-IT#europeanrequirements