- **Oggetto:** Re: POSTA CERTIFICATA: Modello richiesta parere DPO su istanza pervenuta dal Sig. Pietrosanti per conto di Monitora PA
- **Data ricezione email:** 28/04/2023 13:33
- **Mittenti:** Servizio DPO - Gest. doc. - Email: servizio.dpo@afasystems.it
- **Indirizzi nel campo email 'A':** <anic834008@istruzione.it>
- **Indirizzi nel campo email 'CC':**
- **Indirizzo nel campo 'Rispondi A':** Servizio DPO <servizio.dpo@afasystems.it>

Testo email

Gentile Dirigente,
nel seguito di questa email trova le nostre considerazioni sulla email ricevuta all'inizio dello scorso mese di marzo da Monitora PA in merito all'utilizzo dei servizi forniti da Google e Microsoft.

Come è noto, la sentenza Schrems II della Corte di Giustizia dell'Unione Europea del luglio 2020, ha invalidato la decisione di adeguatezza del "Privacy Shield" che costituiva la base giuridica
per un lecito trasferimento di dati personali verso gli Stati Uniti la cui legislazione non garantisce ai cittadini europei una protezione equivalente a quella garantita nell'Unione Europea.
Il Comitato Europeo per la Protezione dei Dati (European Data Protection Board – EDPB), con le Raccomandazioni 01/2020, ha precisato che si possono tuttavia trasferire dati personali verso gli Stati Uniti utilizzando altre basi legali (come le clausole contrattuali standard), ma solo adottando efficaci misure tecniche supplementari.
Di conseguenza l'utilizzo dei servizi offerti da piattaforme che prevedono il trasferimento di dati verso gli Stati Uniti, come le suite Google Workspace e Microsoft 365, è considerato non conforme alle disposizioni del GDPR in assenza di misure tecniche supplementari.

Lo stesso Monitora PA ha fornito chiarimenti circa le misure tecniche supplementari che autorizzerebbero il trasferimento di dati personali verso società statunitensi (https://monitora-pa.it/2023/03/01/gdpr-misure-tecniche-supplementari-efficaci-per-gmail-e-gsuite.html).
Lo scopo di queste misure è quello di rendere tecnicamente impossibile a Google, a Microsoft e, di conseguenza, alle autorità statunitensi l'accesso ai dati personali degli utenti che usano le piattaforme, minimizzandone la diffusione e rendendoli impossibili da ricondurre ai soggetti cui fanno riferimento.
Riportiamo di seguito una sintesi delle misure proposte da Monitora PA:

- *Acquistare per ciascuno studente e ciascun docente un laptop da utilizzare esclusivamente per la connessione scolastica ai servizi di Google. I laptop devono essere privi di circuiteria GSM/4G/5G, possibilmente privi di telecamera, microfono e di software proprietari, disabilitando ogni software o servizio che possa inviare dati verso aziende extra-europee.*
- *Su ogni laptop dovrà essere configurato un singolo account pseudonimico (ovvero con username e password non riconducibili agli assegnatari).*
- *Ad ogni studente (e ad ogni insegnante) dovrà essere assegnato un account pseudonimico per accedere ai servizi di Google o di Microsoft.*
- *Ogni 3 mesi, ogni studente e ogni insegnante dovranno riconsegnare il proprio laptop ai sistemisti che si occuperanno di fornire all'interessato un nuovo laptop e nuove credenziali di accesso ai servizi di Google o di Microsoft.*
- *Configurare una VPN sotto il controllo fisico e amministrativo della scuola che verrà utilizzata come unico punto di accesso ai servizi di Google*

Per facilitare tale procedura Monitora PA consiglia di acquistare un numero di laptop superiore a quello degli interessati (un 40% in più dovrebbe essere sufficiente).

Dovrà poi essere chiaro a tutti gli interessati che non possono utilizzare il proprio nome, il proprio cognome o altro identificativo stabile nelle comunicazioni che transitano attraverso i server di Google o di Microsoft, né potranno essere scambiate informazioni che permettano di identificare univocamente una singola persona (informazioni relative al nucleo familiare, informazioni mediche, scansioni di testi scritti a mano).

Non vi è allo stato dell'arte, un modo compatibile con il GDPR di utilizzare sistemi di video conferenza come Google Meet o Microsoft Teams, che andranno sostituiti con alternative europee cui connettersi tramite hardware distinto dal laptop in questione.

Naturalmente rimane nettamente più rapido ed economico cambiare fornitore. Software liberi come Moodle o NextCloud possono essere acquistati come servizio chiavi in mano da molti fornitori italiani ed europei.

Appare evidente che molte di queste misure sono inapplicabili da parte di una istituzione scolastica e, nonostante la loro complessità, si rivelano tuttavia insufficienti ad una risoluzione completa del problema (restano inutilizzabili, ad esempio, i sistemi di videoconferenza di Google e Microsoft).

Sul tema si è pronunciato anche il Ministero dell'istruzione e del merito che ha inviato il 20 marzo scorso agli USR un documento contenente approfondimenti tecnici sulla valutazione di conformità al GDPR del trasferimento al di fuori dell'UE (in particolare verso gli Stati Uniti) di dati personali degli utenti delle istituzioni scolastiche e dei loro corrispondenti mediante servizi di posta elettronica e piattaforme ICT (link ad ANP, giacché risulta introvabile il link Min. Istruzione: https://www.anp.it/wp-content/uploads/2022/11/approfondimenti_tecnici_di_supporto_per_le_istituzioni_scolastiche_1.0-signed.pdf).
Il documento ribadisce che le istituzioni scolastiche hanno la responsabilità di condurre, in qualità di titolari del trattamento, una verifica di conformità al GDPR del trattamento dei dati personali connessi all'utilizzo delle piattaforme per uso didattico.
Al fine di agevolare tali verifiche, il Ministero segnala alcuni documenti utili ad una prima valutazione (che andrà poi verificata secondo lo specifico contratto sottoscritto e gli specifici dati trattati) e segnala che, tanto Microsoft quanto Google, nella documentazione ufficiale caricata sui rispettivi siti internet dichiarano che il trattamento dei dati, ivi incluso gli aspetti dei trasferimenti transfrontalieri degli stessi, risulta essere conforme rispetto alle norme del GDPR.

Aggiungiamo che la situazione del trasferimento di dati personali verso le big tech con sede negli Stati Uniti è in continua evoluzione:

- Si sta cercando di stipulare un nuovo accordo Usa-Europa (Trans-Atlantic Data Privacy Framework) su cui tuttavia l'EDPB nello scorso febbraio ha espresso ancora perplessità chiedendo chiarimenti su diversi punti (https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en)
- Solo qualche giorno fa, il 26 aprile 2023, in seguito alla pubblicazione sulla Gazzetta Ue del Digital Services Act (Dsa), l'UE ha stabilito che dal 25 agosto le big tech "dovranno cambiare i loro comportamenti" se vorranno restare in Europa. Hanno esattamente quattro mesi di tempo per "rispettare pienamente gli obblighi speciali" previsti dal regolamento Ue (https://www.ansa.it/sito/notizie/tecnologia/hitech/2023/04/26/scatta-la-sorveglianza-della-ue-sulle-big-tech_cd61d7b1-86b2-47ec-ae8e-94f19ad21f22.html)

In conclusione, alla luce delle considerazioni fin qui espresse e considerando inoltre che:

- Difficilmente un Istituto scolastico può dismettere Google Workspace o Microsoft 365 senza patire effetti sulla didattica
- Google Workspace e Microsoft 365 sono servizi SaaS certificati Marketplace AgID (...anche se ciò è irrilevante ai fini del GDPR)

suggeriamo:

- che il Consiglio di Istituto, in rappresentanza di tutti gli interessati (docenti, genitori, studenti), approvi l'utilizzo dei servizi offerti da Google Workspace o Microsoft 365 (specificando i soli servizi effettivamente utilizzati);
- di approvare e diffondere un regolamento di misure facilmente applicabili a cui attenersi per l'utilizzo dei servizi suddetti (ad esempio divieto di utilizzo dei servizi per finalità differenti da quelle didattiche, minimizzazione dei dati personali comunicati tramite i servizi, divieto di trasmissione di foto, ...)
- di **valutare periodicamente** piattaforme e strumenti alternativi per sostituire quelli sopra citati.

Cordiali saluti,
Ing. Michele Petrella
Coordinamento Servizio DPO
AFA Systems

ANIC834008 - A4C9479 - REGISTRO PROTOCOLLO - 0003984 - 28/04/2023 - I.4 - E

Il 22/04/2023 12:49, Per conto di:anic834008@pec.istruzione.it ha scritto:

Messaggio di posta certificata

Il giorno 22/04/2023 alle ore 12:49:00 (+0200) il messaggio "Modello richiesta parere DPO su istanza pervenuta dal Sig. Pietrosanti per conto di Monitora PA" è stato inviato da "anic834008@pec.istruzione.it" indirizzato a:

servizio.dpo@afasystems.it
Il messaggio originale è incluso in allegato.

Identificativo messaggio: 3F91180D.036141DD.A894DCA4.FE57AE57.posta-certificata@legalmail.it

L'allegato daticert.xml contiene informazioni di servizio sulla trasmissione.

Certified email message

On 22/04/2023 at 12:49:00 (+0200) the message "Modello richiesta parere DPO su istanza pervenuta dal Sig. Pietrosanti per conto di Monitora PA" was sent by "anic834008@pec.istruzione.it" and addressed to:

servizio.dpo@afasystems.it
The original message is attached.

Message ID: 3F91180D.036141DD.A894DCA4.FE57AE57.posta-certificata@legalmail.it

The daticert.xml attachment contains service information on the transmission