Ref. Dott.ssa Anna CIMA
Tel. 328.8923614
Email: anna.cima@privacyscuole.it - Pec: anna.cima@legalmail.it

Alla C.A.
del Dirigente Scolastico e del DSGA
e p.c. all'Amministratore della piattaforma/AD

Comunicazione n.6/2023: nota MIM sull'utilizzo dei servizi PEO e delle piattaforme ICT

In relazione alla nota in oggetto, giunta alle scuole in data 21 marzo, si segnala che il Ministero demanda sostanzialmente alle scuole la valutazione di adeguatezza della piattaforma utilizzata (se ne utilizza una).
Nella nota vengono prese in considerazione le dichiarazioni di conformità affermate dai fornitori (Microsoft e Google) e il fatto che il trasferimento dati avvenga sulla base delle **SCC (Clausole Contrattuali Tipo)** sottoscritte tra le parti (Esportatore/Scuola e Importatore/Fornitore), che dovrebbero rappresentare la base giuridica del trasferimento.

A tal riguardo, si ricorda che secondo la **Corte di Giustizia Europea** (con la **Sentenza Schrems-II**) **le SCC non sono sufficienti se il Paese terzo non garantisce lo stesso livello di protezione assicurato all'interno dell'UE**; è quindi necessario esaminare, caso per caso, se la legislazione del Paese terzo assicuri il livello necessario di protezione dei dati personali trasferiti.
Nello specifico, la valutazione di tale livello di protezione deve prendere in considerazione due aspetti:

1) ciò che è stabilito contrattualmente tra l'esportatore dei dati (scuola) stabilito nell'UE e il destinatario del trasferimento (fornitore) stabilito nel Paese terzo;
2) gli elementi del sistema giuridico del Paese terzo e la possibilità di un eventuale accesso da parte delle pubbliche autorità del Paese stesso. Prendendo in considerazione il Paese che riceve i dati (USA), il **Cloud Act** è la legge che permette di fatto l'accesso alle autorità federali statunitensi ai dati raccolti da un Service Cloud di un operatore soggetto al diritto statunitense, anche se i server sono dislocati in paesi terzi rispetto agli USA (es. server Google in Irlanda).

In conclusione, la Corte ritiene che se le Clausole Contrattuali Tipo (SCC) non possono essere rispettate, i trasferimenti di dati personali basati su queste clausole siano sospesi o vietati.
Infatti, essendo le SCC delle clausole contrattuali fra le parti, non possono prevedere garanzie sui diritti degli interessati che impediscano a enti governativi USA di accedere – per motivi di sicurezza – a dati personali memorizzati in datacenter di aziende americane (la norma USA prevale sugli accordi contrattuali tra le parti).

La nota MIM parla poi di **pseudonimizzazione** e **cifratura** dati lato client (cioè aggiuntiva rispetto a quella fornita da Google). Faccio presente ai titolari di trattamento che l'eventuale **crittografia dei dati lato client** si effettua attraverso delle chiavi di crittografia esterne, che si ottengono attraverso due opzioni: utilizzando uno dei partner di Google per i servizi chiavi oppure creando un servizio autonomo di chiavi (nel caso da scegliere e attivare con il supporto e l'intervento del responsabile ICT/amministratore della piattaforma/animatore digitale della scuola) .
In ogni caso, i dati soggetti a criptazione sono file e email, e ciò non è di per sé sufficiente a tutelare gli interessati perché i dati raccolti e trasferiti dalla piattaforma sono molti altri, a partire dal nome

e cognome dell'utente contenuto nell'account nome.cognome@sitoscuola.edu.it, ad altri dati riferiti specificamente allo strumento e alla connessione utilizzata dal singolo utente (indirizzo ip, posizione, informazioni sul dispositivo, informazioni di log, informazioni relative alla rete, ...) per cui ogni misura tecnica messa eventualmente a disposizione dalla e sulla piattaforma, non incide su queste informazioni, perchè ogni singolo utente dovrebbe adottare misure di "protezione" difficilmente attuabili sul proprio device e sulla propria connessione (disattivazione GSM/4G/5G, disattivazione di software e servizi che inviano dati ad aziende extra UE, utilizzo di una VPN dedicata, utilizzo sul device di un account pseudonimizzato non riconducibile al soggetto, ecc...).

Riassumendo:

a) le **SCC (Clausole Contrattuali Tipo)** non sono sufficienti a prevedere garanzie per gli interessati, perché non possono impedire l'attuazione del Cloud Act, e cioè l'accesso da parte degli enti governativi USA ai dati europei memorizzati nei server di aziende americane;
b) la **crittografia dei dati lato client**, attraverso delle chiavi di crittografia esterne, non è sufficiente perché riguarda solo file e email, mentre i dati raccolti e trasferiti dalla piattaforma sono molti altri, a partire dal nome e cognome dell'utente contenuto nell'account nome.cognome@sitoscuola.edu.it, ad altri dati riferiti specificamente allo strumento e alla connessione utilizzata dal singolo utente (indirizzo ip, posizione, informazioni sul dispositivo, informazioni di log, informazioni relative alla rete, ...).

E' opportuno affrontare la questione per step, partendo dalla segnalazione di Monitora Pa sull'utilizzo della PEO di Google. In assenza in tempi brevi del **nuovo accordo UE/USA** (previsto per marzo 2023), sarà opportuno (a opinione della scrivente) **disattivare i DNS Google dal dominio**. Ciò comporterà che gli account del tipo nome.cognome@sitoscuola.edu.it:
- non funzioneranno più come server di posta, quindi non potranno più ricevere e inviare email (ma potranno eventualmente essere riattivati nuovamente quando il problema sarà risolto);
- potranno comunque accedere alla piattaforma di riferimento (es. Google Workspace) per la gestione della stessa e per le operazioni del caso.

Ciò consentirà intanto di ridurre e quindi minimizzare i dati trattati, evitando l'invio di informazioni, comunicazione e documenti tramite la PEO di Google.
Per le email si potranno utilizzare le caselle @istruzione.it per il personale e/o quelle comunicate dagli utenti (del resto l'invio delle email esisteva anche prima di attivare Gsuite), ma si consiglia sempre di **canalizzare le comunicazioni collettive al personale e a famiglie/alunni sul Registro elettronico/Segreteria Digitale**, limitando l'invio tramite email a quelle strettamente necessarie e/o di natura individuale.
Nel caso la scuola non intenda disattivare i DNS Google, dovrà essere nelle condizioni di far fronte, nel breve termine, ad una possibile segnalazione e conseguente accertamento da parte Garante.

Sulla questione più ampia e generale dell'**utilizzo della piattaforma**, sono diversi i possibili scenari:

a) si raggiunge un adeguato accordo UE/USA e si risolve a monte il problema;
b) non si raggiunge l'accordo, e quindi il titolare dismette la piattaforma in quanto il trattamento non è conforme al GDPR;
c) non si raggiunge l'accordo, e il titolare decide di utilizzare ugualmente la piattaforma perché indispensabile.

Ref. Dott.ssa Anna CIMA
Tel. 328.8923614
Email: anna.cima@privacyscuole.it - Pec: anna.cima@legalmail.it

Nel caso c), effettuando la piattaforma trasferimento dati verso un paese terzo per il quale manca una decisione di adeguatezza, il titolare dovrà **valutare il rischio di tale trattamento** e **assumersi la responsabilità dello stesso**. Sarà dunque necessario che il titolare (la scuola):

1) effettui una DPIA e una TIA dalle quali risulti che il rischio per gli interessati (alla luce del quadro sopra esposto) è accettabile;
2) coinvolga eventualmente il Consiglio di Istituto per deliberare l'utilizzo della piattaforma nonostante l'attuale mancanza di adeguatezza;
3) adotti le misure tecniche possibili a minimizzare i dati, con il supporto del responsabile ICT/amministratore della piattaforma/animatore digitale/amministratore di sistema della scuola;
4) imposti la piattaforma con i soli servizi principali escludendo quelli aggiuntivi, con il supporto del responsabile ICT/amministratore della piattaforma/animatore digitale/amministratore di sistema della scuola;
5) individui quali dati trattare tramite la piattaforma (solo quelli strettamente necessari escludendo ogni dato sensibile);
6) informi dettagliatamente tutti gli interessati circa il trattamento dati effettuato dalla piattaforma, del trasferimento dati extra UE e dei rischi correlati.

Mi rendo conto che tale comunicazione, nel complesso, è articolata e con aspetti tecnici forse non immediatamente comprensibili, ma era necessario chiarire alcuni aspetti perché, da un primo vostro riscontro sulla nota MIM, ho percepito da parte di molti una legittima confusione sulla situazione e un approccio "il Ministero ha detto che è conforme e che la posso utilizzare".
E' vero che, in parte, la questione è più formale che sostanziale (perché il problema non è la sicurezza della piattaforma ma il vuoto normativo determinato da Schrems-II), e che è poco probabile l'eventualità che le autorità americane accedano ai dati della scuola, ma sapete che nelle questioni giuridiche e di diritto spesso la forma prevale.

Seguirà una successiva comunicazione per aggiornarvi sull'iter normativo in corso e, nel caso di ritardi sull'adozione del nuovo accordo, si dovrà definire la procedura più adeguata da adottare da parte delle scuole coinvolte.

Resto a disposizione per eventuali chiarimenti.

Data 22/03/2023

Cordiali Saluti
Dott.ssa Anna CIMA