Alla C.A.
Dirigenti Scolastici
Direttori SGA
Sede Istituto

Oggetto: Comunicazione del DPO riscontro alle segnalazioni di MONITORA PA del 01/03/2023 e del 02/03/2023 campagna di segnalazione da parte di Monitora PA con la richiesta di dismettere GMail e Outlook 365

Gentilissimi,
nei primi giorni di Marzo sono arrivate due nuove segnalazioni da parte di **Monitora PA ad oggetto "Segnalazione di trasferimenti sistematici di dati personali verso Google e Microsoft ed il conseguente invito a risolvere la violazione del Regolamento Europeo 2016/679 (GDPR)",** in buona sostanza: dopo le diffide all'uso di Google Analytics, di Google Fonts, del FOIA e dopo i continui monitoraggi dei siti web delle scuole, Monitora PA ha preso sotto il mirino le applicazioni di posta elettronica "G Mail" di Google e "Outlook 365" di Microsoft Corporate.

In cosa consiste la segnalazione di Monitora PA

La segnalazione mette in evidenza quanto segue "*….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*

Tale circostanza può essere verificata tramite l'analisi dei i record MX sul DNS del dominio istituzionale.
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……

Si ricorda che durante la pandemia per poter attivare le piattaforma di comunicazione per la DDI rilasciate da Google (Google Work Space) e da Microsoft (Teams) in forma gratuita le scuole hanno dovuto configurare il record MX per farsi riconoscere come istituto scolastico.
Il record MX è un elemento indispensabile per riceve la posta elettronica.

In data 01/03/2023 Monitora PA invia 3380 PEC ad altrettante Istituzioni Scolastiche con la richiesta di rimuovere entro 60 giorni il servizio di posta elettronica G Mail ed eventualmente ogni altro servizio che determini analoghi trasferimenti, come Google Drive, Google Documents o Google Workspace.
In data 02/03/2023 Monitora PA invia 1121 PEC ad altrettante Istituzioni Scolastiche con la richiesta di rimuovere entro 60 giorni il servizio di posta elettronica di Microsoft Coroporation..- Outlook 365.

Nelle PEC Monitora PA segnala che in alternativa gli Istituti scolastici possono adottare misure tecniche supplementari efficaci alla protezione dei dati personali degli interessati coinvolti nel funzionamento della posta elettronica tali che *"nessun dato, raggiungendo i server di Google e di Microsoft, 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"*.

Nel caso in cui non fossero prese le misure richieste, Monitora PA minaccia di ricorrere al reclamo al garante ai sensi dell'art. 141 del Codice Privacy.

Lo scenario

Monitora PA è un gruppo di attivisti "hacker etici" che per portare avanti la sua battaglia contro i GAFAM (Google, Apple, Facebook, Amazon, Microsoft) sta da tempo prendendo di mira con azioni a tratti vessatorie le pubbliche amministrazioni, ed in particolare le scuole, che dei servizi di queste multinazionali IT si servono per perseguire le proprie finalità istituzionali.

La contestazione di Monitor PA ha origine dalla sentenza **Schrems II** da parte della Corte di giustizia dell'Unione europea (CGUE) che il 16 luglio 2020 dichiara invalida la decisione 2016/1250 della Commissione concernente l'adeguatezza della protezione dei dati personali fornita dal **Privacy Shield**. Questo è un evento di assoluto rilievo, considerato che, fino ad allora la base giuridica correntemente adottata per il trasferimento di dati personali negli USA (e quindi anche l'uso delle piattaforme e dei servizi telematici delle grandi multinazionali statunitensi) era una **decisione di adeguatezza** stabilita proprio dal privacy shield. La sentenza Schrems II ha di fatto preso atto che i programmi di sorveglianza del Governo USA per garantire la sicurezza nazionale (*Cloud Act*) violano i diritti dei cittadini europei sanciti dal GDPR. **Ciò perché la legge consente al governo americano di accedere, per motivi di sicurezza, a qualunque dato personale presente sui server delle aziende statunitensi (anche collocati nel territorio europeo) senza nemmeno avvisare gli interessati, in palese violazione del GDPR.**

Per comprendere la rilevanza dell'evento bisogna considerare che la sentenza ha avuto immediato effetto su più di cinquemila società statunitensi che forniscono i propri servizi a cittadini ed aziende europee e che operavano i loro trattamenti di dati personali sulla base della loro adesione al privacy shield. Se pensiamo che fra queste ci sono aziende come Apple, Google e Facebook è evidente la rilevanza della decisione che si inserisce in un contesto geopolitico di aspro confronto fra UE e USA anche in riferimento al ruolo delle Big Tech.

La prima e più semplice cosa che potevano fare le grandi aziende statunitensi è stata la modifica della base legale dei trattamenti nelle proprie informative che è passata per molte di esse da **"decisione di adeguatezza"** (privacy shield) a **"trasferimento soggetto a garanzie adeguate"** (clausole contrattuali standard). In pratica, aziende come Google, hanno modificato le proprie informative ed hanno inviato ai propri utenti un messaggio in cui si informava che, pur venendo meno il Privacy Shield, il trasferimento dati da UE ad USA poteva ritenersi legittimo perché coperto dalle clausole contrattali standard.

Questo approccio adottato in tutta fretta per consentire l'uso di strumenti ormai di uso quotidiano presenta tuttavia dei limiti che sono stati messi in evidenza da alcune recenti sentenze dei Garanti nazionali. E' quindi oggi necessario un approccio più rigoroso che garantisca, ove possibile,

l'adozione di misure tecniche supplementari a protezione dei dati personali trattati su server collocati al di fuori del territorio Europeo. In ogni caso è richiesto che sia il titolare (il dirigente scolastico nelle scuole) a valutare l'entità dei rischi associati al trattamento dei dati personali su queste piattaforme e a consentire l'uso di esse solo in presenza di rischi che sia possibile contenere al di sotto di una soglia ritenuta accettabile.

Data transfer Ue-Usa, l'Edpb accoglie con riserva il nuovo framework

Secondo l'European Data Protection Board vanno sciolti nodi importanti fra cui la questione della raccolta temporanea di dati in massa e il funzionamento del meccanismo di ricorso. Il presidente Jelinek: "Pur riconoscendo che i miglioramenti apportati al quadro giuridico statunitense sono significativi servono chiarimenti. Necessario anche attuare verifiche almeno ogni tre anni"

Il Comitato europeo per la protezione dei dati (Edpb) ha accolto con riserva il nuovo Data privacy framework (Quadro sulla privacy dei dati) destinato a fornire il quadro giuridico per i flussi di dati transatlantici. L'Edpb, in particolare, accoglie con favore i miglioramenti sostanziali, come l'introduzione di requisiti che incorporano i principi di necessità e proporzionalità per la raccolta di dati da parte dell'intelligence statunitense e il nuovo meccanismo di ricorso per gli interessati dell'Ue. Allo stesso tempo, esprime preoccupazioni e chiede chiarimenti su diversi punti. Questi riguardano, in particolare, alcuni diritti degli interessati, i trasferimenti successivi, la portata delle esenzioni, la raccolta temporanea di dati in massa e il funzionamento pratico del meccanismo di ricorso.

L'Edpb si dice quindi favorevole a subordinare non solo l'entrata in vigore, ma anche l'adozione della decisione all'adozione di politiche e procedure aggiornate per l'attuazione dell'Ordine Esecutivo 14086 da parte di tutte le agenzie di intelligence statunitensi. Al contempo raccomanda alla Commissione di valutare tali politiche e procedure aggiornate e di condividere la propria valutazione con l'Edpb stesso.

Cosa devono fare le scuole?

Il problema è molto complesso e richiede una concreta soluzione che deve essere di natura normativa e politica. Da tempo infatti si sta lavorando ad un nuovo accordo di adeguatezza della protezione dei dati personali fra Unione Europea e Stati Uniti che consentirebbe di operare in tutta tranquillità, ma è ancora in fase di approvazione da parte della commissione EU.

In attesa di sviluppi sul piano normativo (approvazione del nuovo Data privacy framework), **si consiglia**, di comunicare ai propri utenti scuola, che utilizzano i servizi collegati all''account Google e Microsoft di istituto, quanto segue:

- le comunicazioni via email da e per scuola devono avvenire esclusivamente tramite nomeutente@posta.istruzione.it . / meccanograficoscuola@istruzione.it ;
- le comunicazioni con gli alunni e le famiglie devono avvenire, invece, esclusivamente tramite registro elettronico;
- tutti gli utenti devono rimuovere da Google Drive "@scuola.edu.it" di istituto qualsiasi materiale che non sia esplicitamente didattico e che contenga dati personali o sensibili, salvandolo sui propri supporti fisici personali.

In relazione alla misure tecniche adottabili per mettere in sicurezza il servizio di "e-mail" si consiglia di attivare un servizio di **"email security gateway" o un "Relay di posta".**

Un email security gateway è una soluzione che viene utilizzata per proteggere il sistema di posta elettronica dalle minacce informatiche, come ad esempio virus, malware, phishing, spam e altre forme di attacchi informatici.

Il gateway di sicurezza per la posta elettronica è posizionato tra la rete Internet e il sistema di posta elettronica dell'organizzazione, e funge da filtro per il traffico di posta in entrata e in uscita. Questo significa che tutti i messaggi di posta elettronica che passano attraverso il gateway vengono analizzati e filtrati per individuare eventuali minacce informatiche.

Il gateway di sicurezza permette anche di utilizzare più server di posta in base alle esigenze dell'istituto e di inoltrare la posta direttamente alle caselle personali senza dover possedere una casella di posta sul dominio.

È possibile utilizzare anche solamente il **relay di posta** permettendo così ai docenti di avere un alias @dominioscuola.edu.it che rimanda le mail alla propria casella di posta @posta.istruzione.it

Per tutte le altre problematiche si stanno valutando le possibili soluzioni per rendere tecnicamente i servizi compliance.

Con la presente Vi ho voluto fornire alcune informazioni utili a comprendere il contesto in cui ci troviamo ad operare; in base agli sviluppi della vicenda, seguiranno ulteriori comunicazioni.

Nel restare a Vs disposizione vi porgo cordiali saluti

Montecorvino Rovella 12/03/2023

IL DPO

Sandro Falivene

Contatti:

Cell. 333/4207958

E-mail: dpo@info-studio.it

PEC: info-studio@pec.it