All'attenzione del Dirigente Scolastico
dell'Istituto _____
in qualità di soggetto titolare del trattamento ai sensi dell'art. 4 par. 1 n. 7 - GDPR.

Il sottoscritto _____, nato a _____ il _____ (codice fiscale: _____),

- in qualità di docente a tempo indeterminato in servizio nell'istituto scolastico in indirizzo,
- sulla base delle informazioni diffuse e grazie alle attività e al fattivo sostegno degli attivisti del progetto Monitora PA (https://monitora-pa.it),
- eleggendo ai fini del presente atto domicilio fisico in _____ a _____ presso la propria residenza, e domicilio digitale presso la casella PEC _____

1. Ho rilevato che l'istituto scolastico in indirizzo nel quale presto servizio:

- utilizza in via esclusiva per la posta elettronica ordinaria (PEO) dei docenti i servizi forniti da Google,
- utilizza in via esclusiva per la posta elettronica ordinaria (PEO) degli studenti i servizi forniti da Google,
- utilizza in modo maggioritario per la didattica digitale integrata (pur avendo a disposizione dell'istituto la piattaforma Moodle ospitata su server conformi al GDPR e gestiti da personale della scuola) la piattaforma di e-learning Google ClassRoom, e utilizzando Google ClassRoom trasferisce così dati personali, tra i quali la prestazione scolastica ottenuta negli argomenti soggetti a verifica da parte dei docenti, i modelli di verifiche somministrate dai docenti ai propri studenti, i tempi di risposta e la qualità della risposta ai compiti assegnati, ecc., a un soggetto privato senza che siano prese adeguate misure tecniche per anonimizzare i dati oggetto del trasferimento,
- utilizza in alcune occasioni per la gestione e consegna di compiti per casa assegnati agli studenti, le app fornite alla scuole gratuitamente da Google Workspace (come Google Documenti, Google fogli, Google Drive, ecc.) trasferendo così a Google dati relativi al comportamento scolastico degli studenti ed al comportamento professionale dei docenti,
- fa utilizzare ai docenti per le attività funzionali all'insegnamento ex art. 29 CCNL 2007, le app fornite alla scuole gratuitamente da Google Workspace (come Google Documenti, Google fogli, Google Drive, Gmail, ecc.),
- utilizza in via esclusiva per la raccolta delle adesioni ad assemblee sindacali e per altre attività amministrative legate al monitoraggio degli scioperi, la app Google Moduli messa a disposizione gratuitamente da Google Workspace, così fornendo a Google informazioni particolarmente sensibili sul comportamento sindacale dei docenti e degli ATA della scuola, tra i quali la prestazione scolastica ottenuta negli argomenti soggetti a

verifica, a un soggetto privato non ricompreso nell'informativa sulla privacy del vostro istituto.

- utilizza per il ricevimenti individuale/generale dei genitori che vogliano confrontarsi con i docenti dei propri figli (cfr. circolare interna n. 070 del 7/10/2022), la app Google Meet messa a disposizione gratuitamente da Google Workspace, così trasferendo a Google dati sensibili sull'andamento scolastico degli studenti e su eventuali problematiche sanitarie degli stessi, come diagnosi ex legge 104/1992 o ex legge 170/2010,
- utilizza per la gestione e compilazione collettiva dei PDP (Piano Didattico Personalizzato) previsto per gli studenti con diagnosi ex legge 170/2010, e dei PEI (Piano Didattico Individualizzato) previsto per gli studenti con diagnosi ex legge 104/1992, la app Google Documenti messa a disposizione gratuitamente da Google Workspace, così trasferendo a Google dati sensibili sulle problematiche sanitarie degli stessi, compresi gli strumenti compensativi e le misure dispensative proposte dal Consiglio di Classe alle famiglie degli studenti.

2. L'adozione dei servizi sopra elencati forniti da Google e da altri operatori utilizzati dalla scuola per le proprie attività istituzionali, determina **trasferimenti sistematici di dati personali degli utenti (studenti anche minorenni, genitori, docenti), 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 interpersonali
- dati personali descrittivi deducibili dall'incrocio dei dati precedenti, dall'oggetto e dai contenuti dei messaggi trasmessi
- **andamento scolastico di studenti minorenni,**
- **fede religiosa degli studenti iscritti all'insegnamento facoltativo della Religione Cattolica,**
- **comportamento sindacale dei docenti,**
- **situazioni personali anche a carattere sanitario di docenti o studenti,**
- ecc,

3. Le informazioni inviate durante tali trasferimenti, che coinvolgono ovviamente anche persone ignare, in particolare i genitori degli studenti, che decidano di corrispondere con indirizzi email PEO di docenti o studenti dell'istituto scolastico in indirizzo, sono più che sufficienti ad identificare mittenti e destinatari, tracciarne le comunicazioni e ad arricchirne i profili cognitivo-comportamentali in possesso di Google.

È importante infine sottolineare come tali trasferimenti possano includere anche categorie particolari di dati personali, quali quelle oggetto di specifico divieto previsto all'art. 9 comma 1 del GDPR. Si pensi, ad esempio, ai dati relativi alla salute comunicati al personale docente dai genitori o dagli studenti con diagnosi di DSA ex legge 170/2010 o con diagnosi di disabilità ex legge 104/1992.

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 nella UE.

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 dalle analisi effettuate dalle autorità che **il semplice uso di un Cloud Service Provider che sia parte di un gruppo multinazionale** soggetto a normative di un Paese terzo può risultare nell'applicazione delle normative in questione anche **ai dati conservati nello spazio economico europeo.**
Eventuali richieste in tal caso verrebbero direttamente inviate al CSP nel territorio europeo e riguarderebbero dati presenti nel territorio europeo ma non oggetto di trasferimenti già autorizzati. [...]
L'analisi di tutti gli elementi in questione potrebbe portare a **differenti situazioni e differenti violazioni** [...] da parte della pubblica amministrazione stessa se [...] viene ingaggiato un fornitore che non può fornire una protezione adeguata come richiesto dall'articolo 28 comma 1 del GDPR." [^4]

10. Human Rights Watch ha pubblicato nel 2022 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 Google Mail e tutti gli altri servizi già citati che determinino analoghi trasferimenti, come Google Drive, tutte le app di Google Workspace for Education come ad esempio Google ClassRoom, la piattaforma Socrative utilizzata anche per lo svolgimento di verifiche, ed eventuali altre piattaforme utilizzate, per la loro modalità di funzionamento, costituiscono di fatto strumenti di tracciamento e profilazione degli utenti, contrari ai principi e soprattutto alle norme del GDPR, tracciamento per il quale il sottoscritto non ha mai fornito consenso né per sé né per proprio figlio.

13. Tale esteso tracciamento, per il quale come docente sottoscritto non ha mai fornito consenso, non è evitabile in alcun modo perché l'utilizzo di tali strumenti messi a disposizione da parte del datore di lavoro, è sostanzialmente obbligatorio per lo svolgimento delle attività funzionali all'insegnamento ex art. 29 CCNL 2007 attualmente in vigore. Ad esempio per i rapporti individuali con le famiglie di cui al comma 2 lettera c) del già citato art. 29 CCNL 2007, per le comunicazioni organizzative con i colleghi e lo scambio di documenti relativi alle attività collegiali previste, per le comunicazioni con gli studenti, per le comunicazioni con la segreteria, o per fornire informazioni organizzative alla segreteria come ad esempio l'adesione ad assemblee sindacali (rispondendo tramite un Google Moduli predisposto dalla segreteria) oppure per comunicare, sempre rispondendo tramite un Google Moduli predisposto l'intenzione o meno di partecipazione ad uno sciopero.

14. Ritengo quindi che i trasferimenti di dati personali sopra indicati non siano conformi al disposto normativo vigente - in ragione del trasferimento transfrontaliero 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, cioè in particolare **noi docenti, i genitori degli nostri studenti e i nostri studenti anche minorenni a noi affidati.**

15. Pertanto invito il vostro istituto scolastico in indirizzo a voler provvedere alla rimozione dei servizi sopra indicati, entro il termine di 60 giorni dalla ricezione della presente, ad esempio sostituendoli se necessario con servizi analoghi che non violino il GDPR in quanto

sotto il completo controllo fisico e amministrativo di società italiane o europee, anche utilizzando i fondi a disposizione da parte del PNRR - Piano Scuola 4.0.

16. In alternativa e negli stessi termini, invito il vostro istituto scolastico ad adottare misure tecniche supplementari efficaci a protezione dei dati personali degli interessati coinvolti nel funzionamento del Vostro sistema di PEO - inclusi quelli del sottoscritto, coinvolto quale corrispondente di un Vostro indirizzo di PEO - tali che nessun dato (o insieme di dati), raggiungendo i server in questione, 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 presentare reclamo presso l'Autorità Garante per la Protezione dei Dati Personali, ai sensi e per gli effetti dell'art. 77 del Regolamento (Ue) 2016/679 e 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.

Rimanendo a disposizione per ulteriori chiarimenti, colgo l’occasione di porgere distinti saluti.

In fede

_____ , ___/___/_____

Firma

_____

[^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