TRANSFER IMPACT ASSESSMENT (TIA)

Al fine di assicurare l'effettività del principio generale secondo cui il trasferimento dei dati personali verso un paese terzo non deve pregiudicare il livello di protezione delle persone fisiche garantito dal GDPR, gli articoli da 45 a 49 disciplinano vari casi in cui tale trasferimento di dati può lecitamente avere luogo. Limitando l'esame della normativa ai soli casi invocabili dalla P.A., gli articoli rilevanti sono i seguenti:

1. ART. 45 – TRASFERIMENTO SULLA BASE DI UNA DECISIONE DI ADEGUATEZZA

In questo caso, il trasferimento è consentito perché la Commissione Europea ha preso in considerazione e valutato vari fattori del paese terzo (lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, le norme in materia di protezione dei dati, l'esistenza di una autorità di controllo indipendente, gli impegni internazionali assunti in relazione alla protezione dei dati ecc.), decidendo che il paese terzo garantisce un livello di protezione adeguato.

2. ART. 46 – TRASFERIMENTO SOGGETTO A GARANZIE ADEGUATE

L'art. 46 elenca vari elementi che rappresentano "garanzie adeguate" e permettono il trasferimento: quello che rileva, nel caso in esame, è costituito dal fatto che l'importatore dei dati (Google, Microsoft, ecc.) ha aderito a clausole tipo di protezione dei dati (*Standard Contractual Clauses*) adottate da una autorità di controllo ed approvate dalla Commissione Europea secondo una procedura prevista dallo stesso GDPR (art. 93, par. 2).

3. ART. 49 – DEROGHE IN SPECIFICHE SITUAZIONI

Escluse le altre condizioni elencate (come ad esempio il consenso dell'interessato, non applicabile alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri, ai sensi del par. 3 dello stesso art. 49), l'unica astrattamente invocabile nel caso in esame è quella che permette il trasferimento se è necessario per importanti motivi di interesse pubblico.

* * *

Si tratta allora di verificare se il caso concreto, rappresentato dal trasferimento di dati personali verso un paese terzo attraverso l'utilizzo da parte della scuola di piattaforme digitali fornite da provider statunitensi, ricade in una delle situazioni sopra elencate.

LA VERIFICA È NEGATIVA.

Ad onta delle dichiarazioni ufficiali che Google e Microsoft pubblicano sui rispettivi siti internet relativamente alla loro conformità al GDPR, non ricorre alcuna delle condizioni che potrebbero legittimare il trasferimento di dati nei loro confronti.

I motivi sono i seguenti:

1) Mancanza di una decisione di adeguatezza

Come è noto, la sentenza cd. "Schrems II" del 16/07/2020 della Corte di Giustizia dell'Unione Europea ha invalidato il *Privacy Shield* che prima costituiva l'"ombrello" giuridico che rendeva lecito il trasferimento di dati personali dall'Europa verso gli Stati Uniti, ritenendolo non in grado di fornire ai cittadini europei sufficienti garanzie contro le leggi statunitensi in materia di sorveglianza e sicurezza. In pratica, l'ordinamento statunitense non garantisce una protezione dei dati personali equivalente a quella stabilita dal GDPR, poiché le leggi di quel Paese in materia di sorveglianza e sicurezza consentono alle autorità, forze dell'ordine e agenzie di intelligence di acquisire dati informatici dagli operatori di servizi di cloud computing sottoposti alla giurisdizione degli Stati Uniti, a prescindere dal luogo dove i dati si trovano e dagli obblighi contrattuali che gli operatori hanno assunto con i propri clienti. Un eventuale trasferimento di dati personali verso gli Stati Uniti risulterebbe pertanto privo di legittimazione giuridica.

2) Mancanza di garanzie adeguate

Sostanzialmente per la stessa ragione, a nulla rileva il fatto che Google, Microsoft, ecc., abbiano aderito anche alle "nuove" SCC adottate dalla Commissione Europea il 4/6/2021: la clausola 14 dello schema predisposto dalla Commissione richiede infatti alle parti (quindi anche alla P.A. – titolare del trattamento che utilizza la piattaforma) di valutare, prima di concludere le SCC, se le leggi e le prassi del paese terzo di destinazione applicabili al trattamento dei dati personali da parte dell'importatore di dati potrebbero impedire a quest'ultimo di rispettare tali clausole. Tale valutazione del titolare del trattamento non potrebbe che essere negativa, dato che la legge (in questo caso, quella statunitense) prevale sul contratto (che, come si dice, fa stato solo fra le parti che lo hanno stipulato).

3) Mancanza di una condizione derogatoria

L'art. 49, par. 1, lett. d), ammette trasferimento di dati all'estero solo se necessario per "importanti motivi di interesse pubblico". Il considerando 112 elenca alcune ipotesi in cui tale deroga potrebbe trovare applicazione e fornisce una utile guida per la corretta interpretazione dell'aggettivo apposto all'interesse pubblico che legittima un trasferimento di dati ai sensi dell'art. 49: si tratta, ad esempio, di scambio di dati tra amministrazioni fiscali o doganali, scambio di informazioni tra autorità garanti della concorrenza o comunicazione di dati nell'ambito sanitario per esigenze di tutela della salute. Tali indicazioni, ancorché esemplificative, consentono di perimetrare la situazione in cui vi sono interessi collettivi tanto importanti (per usare lo stesso aggettivo dell'art. 49), che prevalgono sulle esigenze di tutela dell'interessato e giustificano un trasferimento di dati pur in assenza di adeguate garanzie. Nel caso dell'utilizzo di piattaforme digitali non è possibile ravvisare simili interessi collettivi prevalenti sulla tutela dell'interessato.

***

Posto l'esito negativo della TIA, la doverosa indicazione del DPO non può che essere quella di sospendere simili trasferimenti di dati personali (in tal caso non è necessario condurre una DPIA ai sensi dell'art. 25 del GDPR).

***

Una DPIA diventa invece necessaria se il Dirigente scolastico ritiene – "t*enendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità*" (art. 32 del GDPR) – di poter mettere in atto "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio" che va, appunto, valutato anche attraverso una DPIA.

Il DPO pur segnalando che, nel caso in esame, il rischio per i diritti e le libertà delle persone fisiche non è del tutto eliminabile, fornisce di seguito indicazioni per la sua mitigazione fino al livello che il titolare del trattamento riterrà accettabile, con la precisazione che alcune di esse sono oggettive (es. pseudonimizzazione) e pertanto – laddove effettivamente implementate – si ritengono approvate dal DPO (ai fini della DPIA), mentre altre dipendono dal comportamento dei singoli (es.: natura e quantità di dati caricati sulla piattaforma); in relazione a queste ultime il DPO può considerarne solo l'utilità pratica ma la garanzia in ordine alla loro reale e diuturna applicazione è demandata al Dirigente scolastico.

D.P.I.A. "DATA PROTECTION IMPACT ASSESSMENT"
VALUTAZIONE DI IMPATTO (DPIA) EX ART. 35 GDPR
INVIO DEI DATI NEGLI USA ATTRAVERSO LE PIATTAFORME GOOGLE E MICROSOFT

BREVE DESCRIZIONE DEL CONTESTO

Per tutte le motivazioni riportate all'interno del protocollo EUservice "come gestire l'invio dei dati in USA", l'utilizzo delle piattaforme Google Workspace for Education e Microsoft 365 Education, di seguito le "piattaforme", suggerite anche da parte del MI all'inizio della DaD, può comportare dei rischi elevati per i diritti e le libertà degli interessati, dovuti al trasferimento dei dati negli USA, qualora tale trattamento non sia ben regolamentato. Pertanto, come menzionato anche negli "Approfondimenti tecnici di supporto per le istituzioni scolastiche" pubblicati dal MI in data 22 marzo 2023 i Titolari del trattamento sono tenuti a condurre una valutazione di impatto (DPIA) ed una verifica di adeguatezza circa le modalità, le garanzie ed i limiti del trattamento dei dati personali nel rispetto della normativa vigente.
Secondo quanto disposto dall'art. 35 del GDPR "*quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e la finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione d'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*". Inoltre "*il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile protezione dei dati, qualora ne sia designato uno*".

Le piattaforme, a prescindere dalla legittimità giuridica, consentono di effettuare i seguenti trattamenti:

- Invio di comunicazioni attraverso il sistema di posta elettronica
- Conservazione degli elaborati in digitale degli alunni
- Trattamento delle categorie particolari di dati personali PEI e PDP
- Conservazione dei dati in cloud
- Dati acquisiti dai moduli
- Utilizzo dei sistemi di videoconferenza

Nella presente valutazione sono state/i considerate/i le principali minacce, le vulnerabilità e i danni derivanti dall'utilizzo delle "piattaforme" per i trattamenti descritti.

VALUTAZIONE DELLA CONFORMITÀ DEI TRATTAMENTI RISPETTO AI PRINCIPI DI CUI ALL'ART. 5 DEL GDPR

In caso di provvedimenti sanzionatori irrogati da parte dell'Autorità, l'art. 5 del GDPR viene quasi sempre menzionato perché in esso sono contenuti i principi portanti del Regolamento.

***Principio di liceità, correttezza e trasparenza*:** è necessario inviare l'informativa agli interessati (alunni, famiglie, dipendenti, fornitori, consulenti e soggetti esterni a vario titolo). A tal riguardo si specifica che non deve essere inviata un'informativa ad hoc nel caso dell'utilizzo delle "piattaforme" perché le informative del Sistema di gestione EUservice già esplicitano che i dati possono essere comunicati ad eventuali ditte fornitrici di altri servizi quali servizi digitali di vario tipo; né tantomeno deve essere richiesto alcun consenso al trattamento, concetto per altro già ribadito dal Garante Privacy nel Provvedimento "Didattica a distanza: prime indicazioni". D'altro canto, va anche sottolineato che non è sufficiente inviare l'informativa per essere *compliant*

al GDPR perché non sarebbe comunque lecito effettuare trattamenti non a norma di legge. Il Dirigente scolastico, infatti, deve essere consapevole di trattare i dati in maniera privacy *compliant* e quindi informare l'utenza in maniera trasparente.

***Principio di limitazione della finalità*:** le "piattaforme", qualora utilizzate, devono essere impiegate per motivi di carattere didattico e amministrativo evitando di utilizzarle per altre finalità rispetto alla didattica (i.e. la consulenza psicologica o il deposito delle foto/video effettuate/i per motivi di carattere non didattico) o per motivi di carattere personale (i.e. utilizzo degli indirizzi di posta elettronica per l'iscrizione a servizi privati).

***Principio di minimizzazione*:** i dati devono essere trattati in maniera strettamente necessaria e indispensabile in relazione alla finalità. Questo principio è applicabile trasversalmente a tutti i trattamenti messi in atto nelle "piattaforme". Pertanto, genericamente dovranno essere trattati il minor numero di dati possibili per tutti i trattamenti elencati nel contesto. In maniera più oculata, bisognerebbe adottare tecniche di anonimizzazione e, ove non possibile, tecniche quantomeno di pseudonimizzazione con cifratura, che non dovrebbe consentire di identificare direttamente gli interessati ma solo attraverso informazioni aggiuntive (i.e. pseudonimi, chiavi di cifratura) in possesso della scuola e, quindi, non messe a disposizione delle "piattaforme".

***Principio di esattezza*:** devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (i.e. non è esatto utilizzare account non più necessari rispetto alla finalità; dovranno quindi essere cancellati account di interessati che hanno abbandonato o che non lavorano presso l'organizzazione).

***Principio di limitazione della conservazione*:** premesso quanto già specificato per il principio di minimizzazione è necessario evitare che i dati eventualmente trattati rimangano conservati nei sistemi in maniera incontrollata. Anche sulla base di quanto disposto dalle "Linee guida sulla DDI" del Ministero la scuola dovrà predisporre sistemi di *repository* evitando di lasciare incustoditi i dati in cloud o all'interno delle aule virtuali. Individuare dei criteri per la conservazione ridurrebbe una parte dei rischi connessi a tale aspetto anche se non eliminerebbe i rischi derivanti da altri trattamenti.

***Principio di integrità e riservatezza*:** la scuola deve mettere in atto misure tecniche ed organizzative adeguate volte a evitare trattamenti non autorizzati o illeciti, la perdita, la distruzione o il danno accidentale dei dati. Essendo le piattaforme statunitensi *cyber resilient* dal punto vista della sicurezza informatica, la scuola deve focalizzarsi prevalentemente sulla corretta definizione delle responsabilità, sulle nomine del team digitale, sulle indicazioni da fornire agli autorizzati compresa la formazione, sull'assegnazione dei privilegi e sul controllo delle vulnerabilità degli account.

Sulla base del *principio di accountability* il Dirigente scolastico è competente quindi per il rispetto di questi principi ed è in grado di comprovarlo.

CALCOLO DEL RISCHIO SUI DIRITTI E LE LIBERTÀ DEGLI INTERESSATI (R) = PROBABILITÀ DI OCCORRENZA DELLA MINACCIA (P) * DANNO (I)

R = P * I

MINACCE

- **Instabilità giuridica sul trasferimento dei dati negli USA**

Questa minaccia comporterebbe allo stato attuale o nel corso del tempo delle problematiche per la riservatezza dei dati dei minori e in generale di tutti gli interessati di cui la scuola tratta i dati all'interno delle "piattaforme" poiché il governo americano potrebbe mantenere o richiedere un accesso "privilegiato" ai dati dei cittadini europei e questi ultimi non potrebbero

"agevolmente" rivolgersi ad autorità competenti locali per esercitare i loro diritti. Pertanto, anche se fosse approvato un nuovo accordo di adeguatezza tra l'UE e gli USA esso potrebbe non soddisfare del tutto i requisiti richiesti dal GDPR con la conseguenza che prima o poi qualche interessato europeo si rivolgerebbe, come già successo con Schrems, alle autorità competenti perché percepirebbe la sua privacy in pericolo. Nel frattempo, i gruppi di attivisti (vedi MonitoraPA) potrebbero continuare ad inviare mail alle scuole mettendo nuovamente in evidenza tutti i rischi del caso. Un quadro, insomma, di costante incertezza circa i mezzi del trattamento utilizzati che non agevolerebbe il lavoro degli istituti scolastici.
È proprio per questo che vi consigliamo caldamente – nel caso continuiate ad utilizzare le "piattaforme" – di mitigare i rischi per i diritti e le libertà degli interessati prendendo in considerazione sia le misure proposte nel nostro protocollo che nella presente DPIA.

- **Attacchi informatici in grado di sfruttare le vulnerabilità delle "piattaforme"**

Sebbene queste "piattaforme" siano sostanzialmente sicure dal punto di vista della *cybersecurity* non si esclude che potrebbero essere oggetto di attacchi informatici quali gli attacchi *ransomware*, una tipologia di *malware* in grado di compromettere la disponibilità dei dati della rete scolastica per esigere in cambio un riscatto generalmente in criptovalute (che non va mai pagato!) e in alcuni casi di causarne l'esfiltrazione. Il *ransomware* potrebbe essere causato da mail ricevute sulla casella di posta contenenti allegati o link malevoli. Il personale potrebbe accidentalmente cliccare sui link e avviare il *cryptolocker* che farebbe esplodere il *malware* andando a cifrare immediatamente tutti i file presenti nella rete. Altri attacchi potrebbero essere dovuti a tecniche di *brute force* in grado di intercettare le password inserite dal personale. Oppure, in senso più ampio, l'organizzazione potrebbe essere oggetto di attacchi *phishing* il cui obiettivo ultimo è quello di adescare l'anello debole della catena attraverso l'installazione di *malware* in seguito, ad esempio, a richieste di verifica di credenziali di accesso a portali e/o servizi esterni (i.e. banche, PagoPA, etc.). I destinatari di queste mail non devono fornire le credenziali richieste né cliccare su eventuali file o link poiché questi comportamenti innescherebbero il *malware*. È tuttavia possibile riconoscere le mail di *phishing* prestando molta attenzione al mittente del messaggio, nonché all'oggetto e al testo della mail.

VULNERABILITÀ

Vulnerabilità di tipo organizzativo	Come risolvere la vulnerabilità
Sono stati aperti gli account dei minori senza averne valutato la reale necessità	Evitare di aprire gli account degli alunni (o se del caso chiuderli) se non ritenuti strettamente indispensabili per la didattica in quanto la stessa potrebbe essere erogata senza problemi attraverso i servizi offerti da parte del registro elettronico
Mancata limitazione dei servizi fruibili dagli utenti attraverso la piattaforma	Impostare la piattaforma con i soli servizi necessari alla didattica (es. Google Drive/One Drive utilizzabili solo per condividere materiali didattici e MAI per documenti contenenti dati personali specie se sensibili, come PEI e PDP) escludendo tutti gli altri servizi (coinvolgendo adeguatamente l'amministratore della piattaforma, l'animatore digitale, l'amministratore di sistema se è stato nominato)
Le persone non autorizzate possono accedere facilmente alle informazioni contenute nelle piattaforme	Implementazione di misure utili a rinforzare la sicurezza dell'identità degli interessati quali *in primis* il cambio password periodico e l'autenticazione a due fattori per gli utenti aventi i privilegi di amministratore della piattaforma

È possibile accedere ai dati appartenenti agli interessati della scuola raccolti all'interno delle piattaforme	Implementazione di procedure di pseudonimizzazione delle comunicazioni, degli account e dei dati personali ivi contenuti o generati mediante tecniche di cifratura dei dati
Assenza di regolamenti	Adozione di regolamenti specifici sul corretto utilizzo delle piattaforme individuando in via formale i dati che possono essere trattati attraverso la piattaforma di riferimento (solo quelli strettamente necessari e MAI quelli sensibili), affinché tutto il personale ne sia consapevole e responsabilizzato.
Mancata nomina del team digitale	Individuazione di personale a cui assegnare le responsabilità sulla privacy derivanti dall'utilizzo delle piattaforme
Non consapevole assegnazione dei privilegi di amministratore	Assegnazione dei privilegi di amministrazione della piattaforma ad utenti con competenze adeguate e limitazione del numero di utenti dotati di tali privilegi
Utilizzo dei pc personali per l'accesso alle piattaforme in assenza di disposizioni specifiche	Invio di indicazioni di *Bring your Own Device* sull'utilizzo dei dispositivi personali
Mancata nomina degli autorizzati	Invio al personale delle lettere di incarico per il trattamento dei dati personali e di istruzioni, compresa la formazione del personale, sul corretto utilizzo delle "piattaforme"
Non reperibilità della nomina di responsabile del trattamento GDPR ex art. 28 sottoscritta con i fornitori delle "piattaforme"	Recupero delle mail di sottoscrizione del contratto di Responsabile del trattamento con le "piattaforme" nonché di sottoscrizione di eventuali emendamenti apportati al contratto (i.e. abbonamenti a pagamento con le "piattaforme"). Si segnala, ad esempio, che nel pannello di amministrazione di Google Workspace, nella sezione "Aspetti legali e conformità" è possibile accedere all'Addendum per il trattamento dei dati Cloud (DPA), che contiene le clausole contrattuali standard e perfeziona la qualifica di Google come responsabile del trattamento.
Mancato controllo sull'utilizzo di applicazioni e servizi aggiuntivi	Implementazione di controlli sui servizi utilizzati attraverso le "piattaforme"
Vulnerabilità di tipo tecnologico	

Assenza di meccanismi di *vulnerability assessment*	Utilizzo di sistemi di *vulnerability assessment* per controllare in maniera sistematica le vulnerabilità connesse all'utilizzo dei singoli account
Vulnerabilità del personale	
Il team digitale non ha competenze di tipo adeguato	Formare il personale sia sull'utilizzo del digitale che sulla privacy

DANNO

L'impatto sugli interessati riguarda soprattutto la violazione della riservatezza dei loro dati potenzialmente derivante dalle minacce sopradescritte. Più la categoria del dato trattata è particolare maggiore sarà potenzialmente il danno per la privacy degli interessati. Le scuole che trattano i dati sensibili quali i PEI o i PDP all'interno delle "piattaforme" andrebbero incontro a danni elevati se non implementassero delle procedure di efficace pseudonimizzazione (es. sostituire mario.rossi@nomescuola.edu.it con A3C16@nomescuola.edu.it , dove la A indica "Alunno", 3C è la classe alla quale appartiene e 16 è il suo numero d'ordine alfabetico nel Registro di classe). Le scuole che utilizzano il sistema di posta delle "piattaforme" per comunicare dati sensibili andrebbero incontro a rischi elevati se non pseudonimizzassero le comunicazioni. Le scuole che creano *repository* per la conservazione degli elaborati andrebbero incontro a danni perlomeno di tipo medio se non implementassero misure di cifratura.

In alternativa, si potrebbero disattivare i DNS Google dal dominio della scuola: tutti gli account del tipo nome.cognome@nomescuola.edu.it non potranno più ricevere e inviare posta elettronica (potranno eventualmente essere riattivati in seguito), mentre potranno comunque accedere alla piattaforma di riferimento per la gestione della stessa o per le operazioni del caso (per la posta elettronica potranno essere utilizzate le caselle @posta.istruzione.it per il personale, e quelle comunicate dagli utenti, limitando comunque l'invio delle sole email strettamente necessarie e di natura individuale, per comunicazioni che non possono essere canalizzate attraverso il Registro Elettronico/Segreteria Digitale).

Tutti questi rischi verrebbero risolti a monte, senza quindi la necessità di adottare particolari procedure di pseudonimizzazione e cifratura ex post, se gli account degli utenti fossero creati in forma pseudonimizzata e se si evitasse di caricare dati sensibili.

Da comportamenti lesivi della privacy degli interessati potrebbero inoltre derivare:

- danni legali per i Titolari dovuti a sanzioni irrogate da parte dell'Autorità Garante per violazione dei principi di cui all'art. 5 del GDPR
- danni reputazionali con risvolto anche di tipo mediatico che porterebbero le famiglie a scegliere altre scuole dove i dati vengono trattati in maniera più sicura

Alla luce di tutto ciò per prevenire o mitigare i rischi messi in evidenza suggeriamo di mettere in atto le misure tecniche ed organizzative descritte nella presente DPIA nonché nel protocollo EUservice "come gestire l'invio dei dati in USA".

Solo con l'adozione delle misure tecniche ed organizzative sopra indicate il Dirigente Scolastico potrà difatti affermare di aver fatto tutto quanto ragionevolmente possibile "*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*", come prescrive l'art. 32 del GDPR.