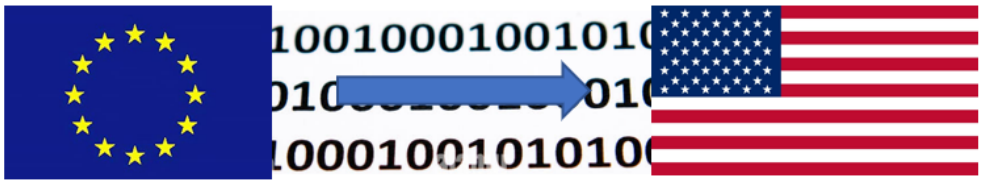
Trasferimento dati in USA, che fare?



Criticità trasferimento dati verso USA, ed altri paesi

La questione verte sull'invio sistematico di dati personali in paese extra-UE, in particolare USA, attraverso servizi e piattaforme delle GAFAM (Google, Amazon, Facebook, Apple, Microsoft), in particolare servizi di posta, repository documentale, piattaforme per videoconferenze e didattica a distanza offerti da Google e Microsoft.

Quali sono le problematiche nel contesto normativo?

Per valutare la trasferibilità dei dati personali verso paesi diversi dall'Unione Europea UE (in realtà Spazio Economico Europeo SEE) vi sono diverse possibilità negli articoli 45, 46, 47 e 49 del GDPR 679/2016:

- un accordo internazionale tra la UE ed il paese extra UE (art. 45);
- l'adesione da parte del ricevente dati a clausole contrattuali standard approvate dalla Commissione Europea (art. 46);
- patti vincolanti di impresa (art. 47);
- consenso al trasferimento (art. 49).

La sentenza *Schrems II* della Corte di Giustizia Europea di fatto **abolisce l'accordo internazionale** tra USA e UE per uniformare la sicurezza del trattamento dati cosi come previsto dal Regolamento Europeo sulla Protezione dei dati (art. 45 del GDPR 679/2016).

Il "Cloud Act" (norma statunitense) mette a rischio anche i dati presenti su server europei di proprietà di società statunitensi, anche se è prevista la possibilità di opporsi alla richiesta di dati motivando opportunamente le ragioni ed utilizzando i contratti sottoscritti.

Allo stato attuale:

- la protezione offerta dall'art. 45 è inapplicabile a causa della sentenza Schrems II;
- la protezione offerta dall'art. 49 è inapplicabile nel mondo della scuola in quanto una Pubblica Amministrazione (PA) non può richiedere Il consenso per il trasferimento dei dati al di fuori dello SEE (art. 49 comma 3);
- molti fornitori di tecnologia, tra cui Google e Microsoft, hanno aderito alle clausole contrattuali standard CCS (art. 46), e ai patti vincolanti di impresa (art. 47), ed alcuni hanno persino dichiarato, nel caso di necessità, di utilizzare il loro staff legale per opporsi all'accesso ai dati per tutela degli interessi dei loro clienti. Hanno anche sottoscritto la

nomina a responsabile esterno al trattamento dati ai sensi ed effetti dell'art. 28 e seguenti del GDPR 679/2016;
- apparentemente esistono le condizioni previste negli art. 46 e 47;
- il Ministero dell'Istruzione e del Merito cita gli atti sottoscritti da Google e Microsoft e rimanda ad una valutazione di impatto (DPIA) che deve effettuare il Titolare con la consulenza del DPO e la decisione su quali strumenti utilizzare. Lo stesso ricorda la possibilità offerta dal PNRR per la valutazione di eventuali soluzioni alternative in CLOUD;
- rimangono punti fermi le raccomandazioni del Garante sull'uso delle piattaforme generaliste per la didattica a distanza, le raccomandazioni dall'EDPB, l'ente dell'Unione Europea che raduna e coordina le diverse Autorità Garanti per la Protezione dei Dati nazionali e la sentenza *Schrems II. Tutto ciò* solleva più di un dubbio sul fatto che le aziende statunitensi possano effettivamente opporsi alla normativa sulla sicurezza nazionale USA ed essere obbligate all'invio di dati alle autorità governative richiedenti dei dati. Questo rappresenta una grave violazione dei principi fondamentali della nostra normativa sulla privacy dove la riservatezza è un diritto fondamentale.

Possibili evoluzioni?

Tutti aspettiamo un Privacy Shield II e di rientrare quindi in quanto previsto nell'art 45 del GDPR 679/2016. Il presidente USA Biden si è mosso in tale direzione ma esiste il problema, di non poco conto, della mancanza di un Regolamento come il nostro che uniformi il trattamento dati tra i vari stati USA. Ciò complica ulteriormente l'accordo tra tutti gli stati USA e l'UE. Senza una regolamentazione complessiva USA il Privacy Shield II potrebbe avere vita breve.

Quali dati personali vengono trasferiti negli USA attraverso le piattaforme?

I dati si possono suddividere in dati di contenuto, dati telemetrici, dati diagnostici e dati legati ai protocolli di trasmissione dei browser, della posta, e degli altri strumenti, come ad esempio l'indirizzo IP e i cookie. Inoltre esiste il problema dell'incrociabilità dei dati. I dati di contenuto possono contenere anche dati particolari (sensibili) se la piattaforma viene utilizzata in modalità non conforme, ad esempio utilizzando lo strumento Google Drive o MS OneDrive per conservare e condividere PEI o PdP.

Quali sono le problematiche nel contesto tecnico ed economico?

I servizi offerti da Google e Microsoft sono efficienti, di facile utilizzo, in molti casi offerti gratuitamente, paradossalmente "sicuri" perché poggiano su infrastrutture che solo società cosi strutturate possono permettersi. Inoltre sono strumenti noti agli utilizzatori. Le loro piattaforme sono qualificate AGID in quanto soluzioni SaaS.

Esistono moltissime alternative open source, quindi gratuite, ma tutte comportano ingenti costi e risorse hardware per il loro utilizzo:

- il costo del server che necessita di molta memoria e potenza di calcolo,
- costo della Banda (velocità e ampiezza di trasferimento dati).

Alcune applicazioni open source potrebbero essere installate con semplicità e gratuitamente sul sito web dell'Istituto, ma Il loro funzionamento sarebbe garantito solo per pochi accessi simultanei. Se volessimo aumentare il numero di utenti contemporanei dovremmo acquistare risorse hardware e di banda cospicue. Le varie soluzioni si differenziano, inoltre, per livelli di efficienza, facilità d'uso, e richieste di risorse.

Quali sono le criticità nel cambiare?

Se la scuola volesse cambiare le attuali piattaforme si troverebbe di fronte alle seguenti criticità:

- Le nuove piattaforme piaceranno ai docenti?
- Ci sarà una perdita parziale delle skills acquisite?
- Comporterà disagi il cambio posta elettronica?
- Occorrerà fare backup di files e posta?
- Occorrerà ricreare gli account per tutti?
- Sarà necessaria tanta formazione per imparare le nuove piattaforme?
- Le prestazioni e la qualità saranno le stesse?
- Quali saranno i costi delle nuove soluzioni?
- Che certezza avremo nel futuro?
- … e ancora altri interrogativi!

Cambierà qualcosa nell'ambito dell'offerta dei servizi Cloud italiani o europei?

I DPO dello staff GDPRistruzione, presupponevano che il MIM fornisse alle scuole una piattaforma dedicata ma l'ultima circolare, dove si consiglia di valutare soluzioni CLOUD con i fondi PNRR, demanda ancora una volta la scelta alla autonomia delle singole istituzioni scolastiche.

Auspichiamo comunque che molte e più funzioni vengano inserite nel registro elettronico che è lo strumento principale da utilizzare.

Comunque è in atto un cambiamento che prevede l'orientamento verso soluzioni in CLOUD per tutte le PA mediante fornitori selezionati, possibilmente nazionali, non extra europei. È già in atto la fase di classificazione dei dati ordinari e strategici, classificazione legata all'importanza degli stessi per la nazione.

Francia, Danimarca e Germania spingono verso soluzioni europee, in cloud e open source, il più possibile uniformi per tutte le scuole.

Quali le possibili scelte:

1) **Lascio tutto così com'è**
2) **Limito l'impatto privacy e utilizzo i sistemi attuali**
3) **Cambio piattaforma**
4) **Chiudo o sospendo le piattaforme in uso**

Scelta 1: Lascio tutto così com'è?

Sicuramente rischiamo di violare il GDPR, non è il caso!

Scelta 2: Limito l'impatto privacy e utilizzo i sistemi attuali

Metto in atto una serie di procedure di natura tecnica e procedurale per escludere alcune tipologie di dati personali, possibilmente spersonalizzandoli e limitando anche l'invio di dati legati ai protocolli di trasmissione e diagnostici, etc.

In tal caso cosa si può fare? Le procedure tecniche per la sicurezza si possono principalmente ricondurre ai seguenti accorgimenti:

1. **Pseudonimizzazione**. È una soluzione che va contro i principi della didattica, ma è un livello di protezione alto e mediando tra sicurezza e didattica si può trovare l'equilibrio.
   La vera pseudonimizzazione, come ha indicato il Garante della Privacy, non è basata sulle iniziali del nome e cognome, o i primi caratteri, o altri pseudonimi attraverso i quali è possibile risalire indirettamente al dato personale.
   Noi suggeriamo di applicare una "pseudonimizzazione di contesto" che consente nell'ambito ristretto dell'istituto scolastico la riconoscibilità del soggetto, ma diventa strumento efficace di irriconoscibilità oltre oceano.

   La pseudonimizzazione deve:

   - Tener conto delle omonimie.
   - Non deve in alcun modo permettere dal dato finale di poter tornare al dato di partenza.
   - Deve permette dal dato di partenza di arrivare sempre allo stesso risultato finale così da agevolare le operazioni di controllo.

   La pseudonimizzazione può essere:

   - **Totale ed univoca tramite hash**, partendo dai dati iniziali es. Mario Rossi nato il 01.01.2010 anno scolastico 22/23 come utente abbiamo alunno.s392143, dando ai docenti il modo di riconoscere i propri studenti con un elenco delle conversioni e la funzione da poter utilizzare quando vogliono per risalire all'utente in piattaforma. **Rischio nullo**
   - **Parziale ed univoca tramite hash** partendo dai dati iniziali es. Mario Rossi nato il 01.01.2010 anno scolastico 22/23 come utente abbiamo mario.s645 avendo già pre-generato le classi dando così ai docenti il modo di riconoscere i propri studenti nelle proprie classi dal nome e dall'hash unico per ogni omonimia. Già l'utilizzo del solo nome porta il **rischio a medio**.
     In questa modalità la didattica non è svilita, resta la praticità e la privacy è assicurata.
   - "**Pseudonimizzazione di contesto**" che consente nell'ambito ristretto dell'istituto scolastico la riconoscibilità del soggetto, ma diventa strumento parziale di irriconoscibilità oltre oceano. Evitiamo pseudonimi tipo alunno1, alunno2, ecc., ma semplicemente usiamo 2/3 caratteri per nome e per cognome, così che Mario Rossi diventi Mar Ros con username mar.ros@scuola.edu.it, consentendo così al docente di identificare l'alunno a cui si rivolge e riducendo il rischio di errori e violazioni privacy per comunicazioni a destinatari errati. In questa modalità la didattica non è svilita, ma il livello porta ad un **rischio medio-alto**.

2. **Abilitare le sole applicazioni strettamente necessarie alla didattica**
   Le piattaforme contengono all'interno tantissime applicazioni abilitate di default, vanno disabilitate tutte ed abilitate solamente quelle strettamente necessarie.
   Ad esempio vanno attivati solamente Classroom/Teams, disabilitata la posta elettronica o restringerla al dominio, disabilitati Moduli/Forms o al massimo da utilizzare solo per le attività didattiche senza utilizzo di dati personali.

3. **Evitare l'uso di DATI PERSONALI e PARTICOLARI (sensibili) nelle piattaforme**
   Quindi no ai PEI e PdP in Drive a meno che non siano pseudonimizzati, no all'uso di Moduli/Forms in cui si raccolgono dati personali, no al salvataggio di foto con volti, nessun dato che permetta la riconducibilità ad una persona fisica. Non far firmare i compiti di Classroom e Teams dagli studenti con nome e cognome, ma utilizzare sempre e solo lo pseudonimo.

4. **Utilizzo di browser che non trasferiscono informazioni.**
   È una soluzione che non ha costo, ma a cui l'utenza si deve adeguare. Permette la navigazione classica senza utilizzo di cookies e altri dati tecnici. Se a questo si aggiunge il non utilizzo del browser della stessa casa della piattaforma si hanno ancora più garanzie.
   Il browser deve garantire alcune misure minime come:
   - Mascheramento o generazione casuale del fingerprint ad ogni accesso;
   - VPN o proxy integrato per nascondere l'IP pubblico di navigazione;
   - Blocco dei traccianti;

- Cookie isolation;
- Cancellazione di cookie, cronologia e password alla chiusura;

5. **Utilizzo di VPN**. L'indirizzo IP dell'utente è un dato personale che permette di identificare il soggetto che naviga, l'area geografica, il fornitore di connettività. Quando si naviga da scuola l'indirizzo IP utilizzato è quello della scuola quindi non più identificativo di un soggetto. Quando non si è a scuola l'indirizzo IP, in genere, diventa identificativo del soggetto. Una possibile soluzione è la fornitura di un sistema che virtualizza la navigazione fornendo al destinatario statunitense un indirizzo IP non associabile al navigatore. Vi sono diversi fornitori di questo tipo di servizio detto tecnicamente VPN.

6. **Nuove modalità di Videoconferenza**
   Le videoconferenze creano ancora più problemi perché la voce ed il volto delle persone sono dati personali difficilmente pseudonimizzabili. Dovremmo suggerire di partecipare alle videoconferenze con microfono e webcam spenti, cosa a dir poco avvilente.
   Cosa possiamo fare?

   - Utilizzo di sistemi di conferenza europei, con base dati in Europa, preferibilmente che si fanno nominare responsabili esterni, in modo da avere la compliance completa!
   - Utilizzo di attuale sistema, con utenti pseudonimizzati di contesto, senza effettuare alcuna registrazione, e senza webcam e microfono, ovvero avvisando gli utenti che i dati potrebbero transitare in paesi in modalità non conforme a GDPR.

7. **Acquisto di versioni a pagamento e componenti aggiuntivi che permettono l'impostazione di criteri sicurezza aggiuntivi e crittografia lato client**
   È possibile innalzare il livello di sicurezza acquistando estensioni alle attuali piattaforme che potrebbero consentire di localizzare i dati in Europa, di attuare sistemi di crittografia (attivazione, configurazione, audit di implementazione, utilizzo della Client Side), e diverse altre opzioni di sicurezza aggiuntive.

Scelta 3: cambio sistema/piattaforma

Le applicazioni in cloud open source, installate su server italiani di provider italiano oppure europeo, certificato AGID, nominato responsabile esterno al trattamento dati, sono la scelta con cui si ha la **compliance massima**. Però ci sono una serie di criticità che abbiamo prima esposto. È fondamentale nella scelta l'avvalersi di società consolidate e strutturate, capaci di intervenire tempestivamente, dotate di risorse umane adeguate, competenza tecnologica, e di capacità finanziaria.

I fondi PNRR possono essere di supporto sia per la strutturazione tecnologica, sia per l'acquisto di servizi, ma anche per la formazione del personale.

Le soluzioni per un cambio sistema/piattaforma sono diverse e potrebbero assumere anche forme ibride come ad esempio l'acquisto di sistemi di videoconferenza da fornitori europei che offrono idonee garanzie, acquisto di risorse in cloud su cui installare applicazioni open source per la didattica e/o repository documentale da altri fornitori che offrono sempre idonee garanzie.

Scelta 4: chiudo o sospendo le piattaforme in uso.

La compliance alla privacy è **totale**! È necessario rimuovere gli account ed i dati prima della chiusura, ovvero pseudonimizzare gli account prima della sospensione. Inoltre docenti ed alunni dovranno eseguire il backup dei loro dati e sostituire gli indirizzi mail ove utilizzati per registrarsi ad ulteriori piattaforme (pensiamo ad esempio ai docenti che hanno utilizzato l'account Google per iscriversi a Canva).

È necessario predisporre la TIA e la DPIA?

Le scelte 3 e 4 (*3.* ***Cambio piattaforma*** *- 4.* ***Chiudo/sospendo le piattaforme in uso***) **non necessitano della redazione di TIA e DPIA** in quanto non si configura più nessun trasferimento dati verso USA.

Le scelte 1 e 2 (*1.* ***Lascio tutto così com'è*** *- 2.* ***Limito l'impatto privacy e utilizzo i sistemi attuali***) **hanno bisogno della redazione della TIA**, compito del Titolare supportato da DPO.

Schema TIA verso USA per le scelte 1 e 2:
(1. Lascio tutto così com'è - 2. Limito l'impatto privacy e utilizzo i sistemi attuali)

Art. GDPR	Situazione attuale	Esito TIA Positivo / Negativo
il trasferimento sia necessario per importanti motivi di interesse pubblico art. 49 comma 1 "Deroghe in specifiche situazioni"	L'interesse pubblico non è supportato dall'attributo necessario (in periodo di pandemia lo era)	Negativo *Ora che è terminato lo stato di emergenza non è possibile addurre questa motivazione.*
Accordo internazionale tra la UE ed il paese extra UE (art. 45);	Decaduto a causa della sentenza Schrems II	Negativo
Consenso al trasferimento (art. 49)	Comma 3: Le PA non possono richiedere consenso per il trasferimento dati Extra UE	Negativo
Adesione da parte del ricevente dati a clausole contrattuali standard approvate dalla Commissione Europea (SCC art. 46);	Si per Google e Microsoft, per altre piattaforme da verificare	Occorre valutazione ulteriore
Patti vincolanti di impresa (art. 47)	Si per Google e Microsoft, per altre piattaforme da verificare	Occorre valutazione ulteriore

La norma prevede che basta anche rientrare in uno degli articoli citati della tabella per consentire il trasferimento dei dati.

Valutazione relativa all'art. 46 - i nuovi SCC dopo settembre 2021.

Per verificare l'applicabilità dell'art. 46 dobbiamo analizzare la clausola 8 della DECISIONE DI ESECUZIONE (UE) 2021/914 DELLA COMMISSIONE del 4 giugno 2021 relativa alle clausole contrattuali tipo.
Clausola 8: Garanzie in materia di protezione dei dati: "*L'esportatore* (la scuola) *garantisce di aver fatto quanto ragionevolmente possibile per stabilire che l'importatore* (Google, Microsoft, altri…)*, grazie all'attuazione di misure tecniche e organizzative adeguate, è in grado di adempiere agli obblighi che gli incombono a norma delle presenti clausole*".

Bisogna soffermarsi sulla frase:"a norma delle presenti clausole" altrimenti si potrebbe essere portati a pensare che le società più strutturate al mondo, dotate di tutte le certificazioni, sicuramente possono adempiere a tutti gli obblighi.

Occorre prestare particolare attenzione alle clausole sulla cooperazione, la nomina, il potere ispettivo, le istruzioni, etc. nei confronti dell'importatore (piattaforme), dalla clausola 8.1 a seguire.

(Il Testo integrale delle decisione della commissione è disponibile qui.)

ESITO DELLA VALUTAZIONE

In base alle valutazioni del Dirigente Scolastico, sentito il DPO, si potranno avere i seguenti esiti:

Il Dirigente Scolastico:	**RITIENE** di poter garantire di aver fatto quanto ragionevolmente possibile per stabilire che l'importatore (Google, Microsoft, altri…), grazie all'attuazione di misure tecniche e organizzative adeguate, è in grado di adempiere agli obblighi che gli incombono a norma delle presenti clausole	**NON RITIENE** di poter garantire di aver fatto quanto ragionevolmente possibile per stabilire che l'importatore (Google, Microsoft, altri…), grazie all'attuazione di misure tecniche e organizzative adeguate, è in grado di adempiere agli obblighi che gli incombono a norma delle presenti clausole
Esito:	**TIA POSITIVA**	**TIA NEGATIVA**

Questa valutazione rende possibile il trasferimento dati verso un importatore specifico di Paese terzo che non ha siglato un accordo internazionale per l'opportunità prevista nell'art. 46.

Negli USA l'arcinota sentenza della Corte di Giustizia Europea sancisce che l'importatore non può sottrarsi ad un obbligo di legge ed essere di fatto costretto a trasferire i dati alle autorità governative, questo pone un problema che va affrontato con una valutazione più approfondita.

Quindi viene richiesto di redigere una DPIA tenendo in considerazione la valutazione di impatto sul rischio per l'interessato relativo al trattamento dati. Per questa valutazione è preferibile concentrarsi su un unico rischio: la motivazione della sentenza Schrems II.

Per la redazione della DPIA risultano utili le FAQ del *COMITATO EUROPEO PER LA PROTEZIONE DEI DATI - EDPB Domande frequenti sulla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 — Data Protection Commissioner/Facebook Ireland Ltd e Maximillian Schrems Adottate il 23 luglio 2020.*

*"**Le misure supplementari unitamente alle SCC, alla luce di un'analisi caso per caso delle circostanze del trasferimento, dovrebbero garantire che la normativa statunitense non interferisca con l'adeguato livello di protezione garantito dalle SCC e dalle misure supplementari stesse.**"*

(Testo integrale sul sito del Garante disponibile qui.)

In queste FAQ (anche se si riferiscono ai vecchi SCC ora abrogati) fonti autorevoli ci forniscono ottime indicazioni su come limitare il rischio e quale è il rischio "accettabile". Purtroppo dovremo prendere in considerazione anche il semplice trasferimento dati e non solo il salvataggio dei dati.

La prima cosa che risalta è che bisogna applicare misure supplementari.

Come si redige una DPIA?

Cerchiamo di fornire elementi utili alla determinazione del livello di sicurezza raggiungibile eseguendo un trattamento dati valutato con sentenza Schrems II su piattaforme in cloud statunitensi.

Per effettuare l'analisi utilizziamo sistemi certificati ISO che incorporano il framework ENISA, strumento per la valutazione del rischio di sicurezza elaborato con il contributo del Garante (clicca per leggere l'articolo sul sito del Garante).

La tabella del rischio in del Framework ENISA è esplicativa. Bisogna rientrare nella zona verde. Partendo da rischio alto e muovendoci nella prima riga della tabella possiamo arrivare al massimo alla zona gialla. Pertanto è necessario applicare misure che facciano ridurre il rischio per consentire il posizionamento nella prima colonna e quindi salire almeno di una casella riducendo le probabilità.

Non possiamo vincolare in alcun modo le autorità governative americane e neppure la probabilità che richiedano dati in base ad una loro decisione.

In una valutazione di impatto non sono ammessi ragionamenti semplicistici del tipo: che interesse hanno le autorità governative americane ai nostri dati? Non li chiederanno mai! Se si potesse ricadremmo nella zona verde.

Di fronte al rischio di violazione del Diritto fondamentale alla privacy i**l titolare deve avere il controllo della situazione**, la DPIA è l'esame minuzioso di elementi pericolosi per i quali attribuiamo un peso alla probabilità che accadano ed al rischio che comportano. La media ponderata ci ubicherà in una zona della tabella in basso, ovvero il resoconto della nostra analisi.

Impatto /probabilità	Basso	Medio	Alto/Molto Alto
Basso			
Medio			
Alto/Molto Alto			

Applicando i principi della privacy la prima cosa che deve fare il Titolare e accertarsi a chi vengono date le informazioni personali e imporre l'obbligo di riservatezza, controllando che venga rispettato.

Il problema di questa particolare analisi è proprio la piattaforma utilizzata. Se inseriamo dati personali diventa estremamente complesso collocarsi nella zona verde in quanto le autorità governative statunitensi potrebbero volerli, potrebbero averli, anche se non sono conservati su server europei.

È possibile, ed occorre, ridurre il livello di pericolosità riducendo il rischio.

Purtroppo solo con alcune delle contromisure attuabili possiamo garantire la zona verde.

Facciamo un esempio basato sull'uso della posta elettronica fornite dalle piattaforme. Senza alcun intervento tecnico ricadiamo nella zona rossa.

Possiamo migliorare attraverso contromisure:

- Non si usa la posta elettronica di Google/Microsoft ma si usa quella del Ministero = (zona verde).
- Si bloccano le mail di Google al dominio interno così almeno non escono fuori dell'Istituto applicando la pseudonimizzazione = (zona gialla)**.**

Quindi nel caso di utilizzo di Piattaforme Google/Microsoft:

- è assolutamente necessario allontanarci dalla zona rossa applicando le contromisure. (questo anche a prescindere dalla Sentenza Schrems II);
- Non avendo il controllo completo, cioè la possibilità di "blindare", per i protocolli di trasmissione della posta e dei browser, applicando tutte le misure indicate in precedenza riusciamo a ricadere nella zona gialla (stima 80%);
- Il titolare che effettua la Valutazione ha una chiara rappresentazione del rischio e procede ad una ulteriore analisi che completa la DPIA.

A Seguito della Valutazione di impatto:

- se il valuto il **rischio troppo alto** chiudo/sospendo le piattaforme e/o scelgo altre alternative alle piattaforme in uso.
- se il valuto il **rischio alto** attuo soluzioni ibride, cambio il sistema di scambio file, di forms, di sondaggi, con sistemi open source e/o sistemi di videoconferenze compatibili con la privacy e/o uso le piattaforme statunitensi per attività prettamente legate alla didattica sensibilizzando gli utenti ad un uso consapevole e/o utilizzo sistemi open source.

Valutato il rischio, per assicurare un servizio pubblico migliore, considerato pure lo stato dell'arte (art.32), tenuto conto dei costi di transizione verso soluzioni diverse da quelle in uso, ed in generale per motivi di efficienza, di economicità, e quant'altro, in attesa di un probabile nuovo accordo internazionale, attuo le seguenti contromisure... e sensibilizzo gli utenti ad un uso consapevole delle piattaforme in uso.

Suggeriamo, inoltre, di valutare attentamente le affermazioni, anche di DPO, troppo semplicistiche: *è tutto ok, possiamo fare tutto, non ci sono violazioni, il Garante non commenerà mai una sanzione, stiamo operando per rilevante interesse pubblico, così fanno tutti, così fanno i ministeri, non si può fermare la tecnologia, questi attivisti non hanno nulla da fare…*

In questi giorni ne sono circolate tante! Se fosse stato così semplice ce lo avrebbe segnalato sia il MIM, sia il Garante, sia Google, sia Microsoft.

Google propone un video per approfondire la tematica in cui ritroviamo un'analisi puntuale (link video Google).

Bisogna sempre considerare che potremmo essere chiamati a giudizio. In quella sede non c'è stato nessuno scrupolo a sollevare un problema planetario per sancire che la privacy è un diritto fondamentale per gli europei e non lo è per gli statunitensi. Se possibile occorre documentare le scelte adottate evidenziando che tengono conto della sentenza, di indagini di mercato, di test

sulla efficienza di soluzioni alternative, di valutazioni sull'attuazione di transizioni progressive verso soluzioni alternative predisponendo percorsi formativi e quant'altro riterrete opportuno.

In merito alla documentazione richiesta da più scuole:

L'esemplificazione di TIA, in pratica, è fornita in questo articolo che vi consente di individuarne l'esito positivo o negativo!

L'esemplificazione della DPIA vi consente di individuare le misure da attuare in caso di TIA positiva.

È stato predisposto uno schema delle misure di sicurezza riportante impatto e probabilità, corredato dai colori rosso, giallo, verde per ogni singola scelta in modo da essere agevolati nell'adozione delle contromisure.

A breve in area riservata i modelli, gli schemi e la documentazione da poter diffondere, bozza delle circolari per l'attuazione delle scelte.

Restiamo disponibili, in funzione delle vostre scelte formalizzate, a darvi supporto per la redazione di TIA e DPIA.

Dott. Valentino Valente - Attilio Milli - Staff GDPRistruzione.it

Con la collaborazione dei DPO Giovanni Fiorillo, Sandro Maini, Vincenzo Monteforte, Roberta Tomeo, Sandro Falivene, Luca Maletta, Antonio Bove, Edoardo Duilio.