EUSERVICE

Presenta:

DIDATTICA A DISTANZA

SCEGLIERE LA PIATTAFORMA SENZA INVIARE DATI IN USA

GUIDA PRATICA

Presentato da
EUservice

Supervisione
Angelo Leone

Con la collaborazione di
Diego Dimalta

OTTOBRE 2020

EUSERVICE

INDICE

EUSERVICE

INTRODUZIONE

DEFINIZIONI

La scelta della piattaforma per la didattica a distanza non è mai stata semplice.

I recenti avvenimenti, che approfondiremo infra, hanno purtroppo reso questo adempimento ancora più arduo.
Prima di procedere oltre, al fine di meglio comprendere le vicende di cui parleremo, è utile però effettuare una premessa che fornisca le definizioni di alcuni termini a cui faremo frequente riferimento nelle prossime pagine.

In primo luogo è utile evidenziare come, in base al GDPR, il trasferimento di dati al di fuori dello spazio UE è tendenzialmente vietato salvo il ricorrere di alcune condizioni. Le soluzioni adottate più frequentemente sono:

DECISIONE DI ADEGUATEZZA (45 GDPR): Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo in questione garantisce un livello di protezione adeguato.

CLAUOSLE CONTRATTUALI STANDARD (46 GDPR): La Commissione Europea o l'Autorità di controllo competente previa approvazione della Commissione può stabilire che determinati strumenti contrattuali consentano di trasferire dati personali verso Paesi terzi o organizzazioni internazionali.

Una soluzione che si poneva come via di mezzo tra le due citate era il **PRIVACY SHIELD**: accordo che regolamentava il trasferimento di dati tra Unione europea e USA. L'accordo mirava a proteggere i diritti fondamentali delle persone nell´UE i cui dati personali venivano trasferiti negli Stati Uniti, e stabiliva regole certe per le imprese che effettuavano trasferimenti di dati al di là dell´Atlantico.
Il PRIVACY SHIELD è stato annullato il 16 Luglio 2020 a seguito della sentenza Schrems II.

Perché ci interessa?
Perché la maggior parte delle grandi società che operano in Internet (le "Big tech") inviano dati in USA in forza di PRIVACY SHIELD o di CLAUSOLE CONTRATTUALI STANDARD (CCS).

EUSERVICE

SCENARIO ATTUALE. SHREMS II

La Corte di giustizia dell'Unione europea (CGUE) il 16 luglio 2020 ha pronunciato la c.d. "Sentenza Schrems II" affrontando il tema del trasferimento dei dati tra l'Unione europea e gli Stati Uniti.

Nell'ambito di questa sentenza la Corte ha invalidato il PRIVACY SHIELD rendendo quindi illegittimo l'invio di dati in USA basato su questa modalità semplificata.

Non solo, la Corte si è pronunciata anche sulle CLAUSOLE CONTRATTUALI STANDARD precisando che le stesse potranno continuare ad essere utilizzate ma **solo in presenza di GARANZIE ULTERIORI.**

Questa decisione ha avuto conseguenze molto importanti in quanto le "Big Tech" hanno dovuto adeguarsi non potendo più fare affidamento sul PRIVACY SHIELD.

Il problema. però è che molte di loro, anziché spostare i server in UE (come avrebbe voluto la Corte) hanno preferito restare in USA e fondare il trasferimento dati sulle CLAUSOLE CONTRATTUALI STANDARD.

Il problema è che, purtroppo, come abbiamo visto, le CCS secondo la Corte possono essere utilizzate solo in presenza di MISURE ULTERIORI. Differentemente, in mancanza di tali accorgimenti, il trasferimenti in USA è da ritenersi illegittimo.

Questo passaggio le "Big Tech" paiono averlo totalmente ignorato e, pertanto, l'utilizzo dei loro servizi risulta potenzialmente pericoloso.

Non a caso l'Autorità Garante irlandese ha di recente intimato a Facebook di spostare tempestivamente i suoi server in Unione Europea minacciando, sanzioni sino al 4% del fatturato globale.

In questo scenario difficile si colloca la scelta del sistema per la didattica a distanza che ogni scuola deve compiere di concerto con il proprio DPO.

Sistemi che fino a "ieri" erano considerati sicuri, anche da AGID" sono diventati rischiosi e la scuola potrebbe essere chiamata a rispondere per l'utilizzo degli stessi.

EUSERVICE

INDICAZIONI UFFICIALI

EUSERVICE

F.A.Q. DEL GARANTE PRIVACY

PREMESSA:
Il Comitato Europeo per la Protezione dei Dati (EDPB) ha predisposto delle FAQ relative alla sentenza Schrems II e ai suoi effetti. Queste sono solo alcune delle domande tradotte dal Garante Privacy italiano. La versione integrale è reperibile sul sito www.garanteprivacy.it.

Che cosa ha stabilito la Corte nella sua sentenza?
[...] La Corte ha ritenuto che i requisiti del diritto interno degli Stati Uniti, e in particolare determinati programmi che consentono alle autorità pubbliche degli Stati Uniti di accedere ai dati personali trasferiti dall'UE agli Stati Uniti ai fini della sicurezza nazionale, comportino limitazioni alla protezione dei dati personali che non sono configurate in modo da soddisfare requisiti sostanzialmente equivalenti a quelli previsti dal diritto dell'UE1 e che tale legislazione non accordi ai soggetti interessati diritti azionabili in sede giudiziaria nei confronti delle autorità statunitensi. Alla luce di tale grado di ingerenza nei diritti fondamentali delle persone i cui dati sono trasferiti verso il suddetto paese terzo, la Corte ha dichiarato invalida la decisione sull'adeguatezza dello scudo per la privacy (Privacy Shield).

È previsto un periodo di grazia durante il quale continuare a trasferire i dati verso gli USA senza valutare la base giuridica per il trasferimento?
No, la Corte ha annullato la decisione relativa allo scudo per la privacy senza preservarne gli effetti, in quanto la normativa americana che è oggetto di valutazione da parte della Corte non fornisce un livello di protezione sostanzialmente equivalente a quello dell'UE. Tale valutazione deve essere tenuta presente con riguardo a ogni trasferimento verso gli Stati Uniti.

EUSERVICE

F.A.Q. DEL GARANTE PRIVACY

Che cosa posso fare per continuare a utilizzare i servizi del mio responsabile del trattamento [es. PIATTAFORMA D.A.D. ndr] se il contratto firmato a norma dell'articolo 28, paragrafo 3, RGPD indica che i dati possono essere trasferiti verso gli USA o verso un altro paese terzo?

Se è previsto che i dati siano trasferiti verso gli Stati Uniti e non possono essere introdotte misure supplementari per garantire che la normativa statunitense non incida sul livello di protezione sostanzialmente equivalente a quello offerto nel SEE assicurato dagli strumenti di trasferimento, né si applicano le deroghe di cui all'articolo 49 del RGPD, l'unica soluzione è negoziare un emendamento o una clausola aggiuntiva al contratto per vietare il trasferimento di dati verso gli USA.
Non solo la conservazione, ma anche la gestione dei dati dovrebbero quindi avvenire in paesi diversi dagli USA. è Se è previsto che i dati siano trasferiti verso un altro paese terzo, occorre analizzare anche la legislazione di tale paese terzo per verificarne la conformità ai requisiti della Corte e al livello di protezione dei dati personali atteso.

Se non è possibile individuare un'idonea base giuridica per il trasferimento verso un paese terzo, **non dovrebbe aver luogo alcun trasferimento di dati personali al di fuori del SEE (Spazio Economico Europeo) e tutte le attività di trattamento dovrebbero aver luogo all'interno del SEE.**

EUSERVICE

LINEE GUIDA DELL' AUTORITÀ TEDESCA

Come visto, la sentenza Schrems II ha causato molti disagi dovuti in parte anche alla confusione venutasi a creare per la mancanza di indicazioni certe da parte delle Autorità di Controllo (i Garanti Privacy europei, per capirci).

Le uniche indicazioni ufficiali arrivano dall'Autorità Tedesca la quale, in data 25 Agosto 2020 èha pubblicato delle linee guida molto utili anche per gli altri stati europei essendo il GDPR applicabile in modo uguale in tutta Europa.

L'Autorità, dopo aver eseguito un rapido excursus della vicenda, è entrata nel merito precisando quanto segue.

1.*Sebbene, in prima istanza, la sentenza della Corte di Giustizia Europea abbia un effetto meramente inter partes, è da evidenziare come, di riflesso, essa vincoli tutte le Autorità e Tribunali degli Stati membri. Non solo, se la Corte di giustizia europea dichiara invalido un atto comunitario (come il PRIVACY SHIELD), tutti i Tribunali e le Autorità di tutti gli Stati membri sono vincolati e quindi obbligati a disapplicarlo.*

2.*La sentenza Schrems II ha effetti, tre l'altro sui seguenti servizi:* **SERVIZI ARCHIVIAZIONE DATI** (CLOUD) *e* **SISTEMI DI VIDEOCONFERENZA.**

3. *Come comportarsi quindi? Se devi trasferire i dati un USA devi utilizzare i seguenti accorgimenti:*

- UTILIZZO DELLE CCS (POSSIBILMENTE MODIFICATE COME DA INDICAZIONI)
- CRITTOGRAFIA CON CHIAVE IN UE
- ANONIMIZZAZIONE
- PSEUDONIMIZZAZIONE CON CHIAVE IN UE

La versione integrale delle linee guida (in lingua tedesca) può essere rinvenuta all'indirizzo www.baden-wuerttemberg.datenschutz.de

LA NOSTRA SOLUZIONE

PROTOCOLLO EUSERVICE

PROTOCOLLO EUSERVICE

FARE UNA SCELTA

Alla luce di tutto quanto sopra evidenziato le scuole hanno due opzioni:

1- SCEGLIERE UNA PIATTAFORMA ITALIANA O EUROPEA

2- CONTINUARE AD USARE LE PIATTAFORME USA AVENDO CURA DI RIDURRE SENSIBILMENTE IL RISCHIO

OPZIONE 1
PIATTAFORME ITALIANE

Esistono diverse società che garantiscono la possibilità di utilizzare piattaforme con server in Italia o in Europa. E' però importante che tale possibilità non sia meramente di facciata come abbiamo già rilevato in alcuni casi.

Per questo, prima di procedere al cambio piattaforma si consiglia di consultare il DPO e di leggere attentamente l'informativa, eventualmente chiedendo precisazioni al DPO della società distributrice della piattaforma.

OPZIONE 2
RIDURRE IL RISCHIO

L'utilizzo di piattaforme statunitensi è pericoloso solo laddove le stesse vengono utilizzate per archiviare o inviare dati personali (nome, cognome, immagini, indirizzi e mail ecc ecc).
Se la piattaforma viene utilizzata in modo da evitare il trattamento di tali dati, allora il rischio risulta praticamente nullo.

Diventa quindi essenziale affidarsi ad un DPO capace di fare ricorso a tutte le soluzioni utili previste dalla normativa sulla data protection e dalle prassi più accreditate.

Nelle prossime pagine forniremo una serie di suggerimenti diretti dapprima a gestire i rapporti tra il personale scolastico e, infine, a gestire i rapporti tra docenti/ATA e studenti.

PROTOCOLLO EUSERVICE

RAPPORTI INTERNI AL PERSONALE

ATTIVITÀ

Invio e-mail **prive** di dati personali **nel corpo messaggio**.

RISCHIO

Se il documento NON contiene dati personali, l'unico rischio è quello relativo all'utilizzo di indirizzi e-mail dai quali si evincano nome e cognome del mittente o del destinatario.

SOLUZIONE PROPOSTA

Utilizzare indirizzi e-mail diversi da nome.cognome@scuola.it
Ad esempio, l'indirizzo potrebbe essere n.c.@scuola.it (ancora meglio se del tipo "docenti.classe2A@scuola.it).
In ogni caso il suggerimento è quello di usare indirizzi mail ospitati sul server (UE) del sito della scuola evitando quindi e-mail generate da servizi americani.

ATTIVITÀ

Invio mail **contenenti** dati personali **nel corpo messaggio.**

RISCHIO

Se il documento contiene dati personali (oltre all'indirizzo e mail), qualora si utilizzino servizi e-mail statunitensi, gli stessi potrebbero non essere adeguati alla normativa UE, mettendo quindi in pericolo la riservatezza dei dati di studenti e colleghi.

SOLUZIONE PROPOSTA

Utilizzare servizi e-mail con server in Unione Europea (o in stati ritenuti adeguati dalla UE) evitando quindi i servizi statunitensi tipo Gmail e simili.
Nella maggior parte dei casi il sito della scuola è ospitato su server UE, per questo motivo potrebbe essere consigliabile utilizzare e-mail ospitate sul dominio di tale sito scolastico.
Se, nonostante tutto, si preferisce continuare ad utilizzare servizi americani, è necessario che nel corpo messaggio non si faccia in alcun modo riferimento a persone identificate o identificabili.

PROTOCOLLO EUSERVICE

RAPPORTI INTERNI AL PERSONALE

ATTIVITÀ	RISCHIO
Invio mail **contenenti** dati personali **negli allegati.**	Se la mail con dominio Gmail e simili viene utilizzata per l'invio di allegati/documenti contenenti informazioni sullo studente o su altri docenti, questo potrebbe provocare grossi problemi per la riservatezza dei dati di studenti e colleghi.
	SOLUZIONE PROPOSTA
	Utilizzare servizi e-mail con server in Unione Europea (o in stati ritenuti adeguati dalla UE) evitando quindi i servizi statunitensi oppure utilizzare un server a scuola con diverse cartelle accessibili ai docenti/ATA in base alla classe. Se si vuole continuare ad utilizzare servizi americani, allora è necessario che i documenti siano epurati da ogni riferimento a persone identificate o identificabili.

ATTIVITÀ	RISCHIO
Deposito documenti su **cloud.**	Se il cloud ha sede in paesi diversi dalla UE (o da quelli considerati adeguati) è possibile che tale condotta comporti un grosso pericolo per la riservatezza dei dati di studenti e colleghi.
	SOLUZIONE PROPOSTA
	Utilizzare cloud con sede in Unione Europea oppure utilizzare un server a scuola con diverse cartelle accessibili ai docenti/ATA delle diverse classi. Il collegamento dovrebbe avvenire preferibilmente con VPN. Il cloud americano potrà essere utilizzato solo per depositare documenti privi di riferimento alcuno a persone identificate o identificabili. Infine, in via residuale, è concesso l'utilizzo di servizi americani per depositare documenti NON anonimi, ma solo previa cifratura con chiave segreta o, comunque, non comunicata tramite servizi americani.

PROTOCOLLO EUSERVICE

RAPPORTI INTERNI AL PERSONALE

ATTIVITÀ	RISCHIO
Riunioni da remoto in **video conferenza.**	Secondo le linee guida dell'Autorità Tedesca, anche l'utilizzo di sistemi di video conferenza con server in USA può arrecare pericolo ai dati.

SOLUZIONE PROPOSTA

L'unica soluzione capace di azzerare il rischio è quella di utilizzare sistemi con server in UE.
Differentemente, al solo scopo di ridurre il rischio, il suggerimento è quello di usare sistemi che si garantiscano cifratura end to end.

Sarà poi opportuno evitare di utilizzare il proprio nome per identificarsi durante la call, preferendo invece degli pseudonimi se non addirittura dei codici. Infine, quanto alle immagini, sarebbe preferibile spegnere il video o, comunque accenderlo per brevi momenti.

ATTIVITÀ	RISCHIO
Utilizzo di sistemi di **messaggistica.**	In generale è sconsigliato l'utilizzo di sistemi di messaggistica. Qualora ciò fosse concesso dal dirigente, se nei messaggi con i colleghi dovessero essere contenuti dati personali è possibile che da ciò derivi un rischio per la riservatezza delle informazioni di studenti e colleghi.

SOLUZIONE PROPOSTA

La soluzione migliore è quella di evitare sistemi di messaggistica.

Qualora ciò non fosse possibile, il consiglio è quello di omettere l'indicazione di dati personali di studenti o di colleghi i quali potranno essere identificati in un secondo momento oppure mediante uno pseudonimo o un codice.

PROTOCOLLO EUSERVICE

RAPPORTI SCUOLA/ALUNNI

ATTIVITÀ	RISCHIO
Invio **tracce** per i compiti.	Le tracce non contengono riferimenti diretti a studenti. Il rischio è quindi praticamente nullo.
	SOLUZIONE PROPOSTA
	Evitare di inserire nelle tracce riferimenti o comunque dati capaci di identificare o rendere identificabile uno studente.

ATTIVITÀ	RISCHIO
Ricezione **compiti/ e-mail** dagli studenti.	La ricezione di e-mail da parte degli studenti ha due criticità: 1-nell'indirizzo mail potrebbero esserci nome e cognome degli studenti; 2- nel corpo e negli allegati potrebbero esserci dati personali degli studenti.
	SOLUZIONE PROPOSTA
	La scuola dovrebbe utilizzare sistemi mail o cloud con server in UE (vedere pagine precedenti) oppure un server a scuola con diverse cartelle accessibili agli studenti delle diverse classi. Il collegamento dovrebbe avvenire preferibilmente con VPN. Se ciò non è possibile allora è necessario che gli studenti utilizzino mail prive di riferimento a nome e cognome. Inoltre è necessario che i compiti non contengano dati personali i quali potrebbero, ad esempio, essere sostitutiti da codici.

PROTOCOLLO EUSERVICE

RAPPORTI SCUOLA/ALUNNI

ATTIVITÀ	RISCHIO
Lezioni a distanza/ in **video conferenza.**	Secondo le linee guida dell'Autorità Tedesca, anche l'utilizzo di sistemi di video conferenza con server in USA potrebbe arrecare pericolo ai dati.

SOLUZIONE PROPOSTA

L'unica soluzione capace di azzerare il rischio è quella di utilizzare sistemi con server in UE.
Differentemente, al solo scopo di ridurre il rischio, il suggerimento è quello di usare sistemi che garantiscano cifratura end to end.

Sarà poi opportuno ricordare agli studenti di non utilizzare il proprio nome per identificarsi durante la call, preferendo invece degli pseudonimi, se non addirittura dei codici. Infine, quanto alle immagini, sarebbe preferibile spegnere il video o, comunque accenderlo per brevi momenti.

ATTIVITÀ	RISCHIO
Deposito documenti su **cloud e piattaforme edu.**	L'utilizzo di sistemi cloud e piattaforme edu presenta due criticità: 1- per accedere è necessario creare un account (solitamente usando indirizzo mail); 2- i documenti depositati potrebbero contenenere dati personali.

SOLUZIONE PROPOSTA

La scuola dovrebbe utilizzare sistemi cloud con server in UE (vedere pagine precedenti)oppure un server a scuola con diverse cartelle accessibili agli studenti delle diverse classi. Il collegamento dovrebbe avvenire preferibilmente con VPN.
Se ciò non è possibile allora è necessario che gli studenti utilizzino per iscriversi mail prive di riferimento a nome e cognome.
Inoltre è necessario che i documenti condivisi non contengano dati personali i quali potrebbero, ad esempio, essere sostitutiti da codici.

PROTOCOLLO EUSERVICE

RAPPORTI SCUOLA/ALUNNI

ATTIVITÀ	RISCHIO
Utilizzo sistemi per **messaggi scuola/famiglia.**	In generale è sconsigliato l'utilizzo di sistemi di messaggistica per le comunicazioni scuola/famiglia. Qualora ciò fosse concesso dal dirigente, se nei messaggi dovessero essere presenti dati personali è possibile che da ciò derivi un rischio per la riservatezza delle informazioni di studenti e colleghi.

SOLUZIONE PROPOSTA

La soluzione migliore è quella di evitare sistemi di messaggistica.

Qualora ciò non fosse possibile, il consiglio è quello di omettere l'indicazione di dati personali di studenti i quali potranno essere identificati in un secondo momento oppure mediante uno pseudonimo o un codice.

ATTIVITÀ	RISCHIO
App complementari al sistema di conference call.	Solitamente le app complementari richiedono la creazione di account tramite l'indirizzo mail degli studenti. In alcuni casi le app trattano anche altri dati personali.

SOLUZIONE PROPOSTA

Se la app ha server in UE non ci sono problemi.
Se la app ha server fuori dalla UE allora si procede come segue: se la app richiede l'indirizzo e-mail degli studenti, è opportuno che ogni studente si doti di un indirizzo e-mail privo di riferimenti al nome e cognome.
In ogni caso è necessario che lo studente non invii dato alcuno alla app.

EUSERVICE

INDIRIZZO

Via Dante Alighieri, 12 - 00027 Roviano (RM)

EMAIL

info@euservice.it

NUMERI DI TELEFONO

Ufficio Consulenza 0774.903270
Ufficio Formazione 06.7232251
Ufficio Privacy 06.92929166

SEGUICI SUI NOSTRI CANALI