**Ref. Dott.ssa Anna CIMA**
Tel. 328.8923614

**Alla C.A.**
**del Dirigente Scolastico e del DSGA**

## Comunicazione n.18/2023: nuovo accordo UE-USA sul trasferimento transatlantico dei dati (il Data Privacy Framework) e documenti necessari.

In data 10 luglio 2023, dopo tre anni di attesa e di vuoto normativo, **è stato finalmente approvato il nuovo accordo UE-USA sul trasferimento transatlantico dei dati, il UE-U.S. Data Privacy Framework**, entrato ufficialmente in vigore in data 11 luglio 2023.

Come ormai sapete, a seguito della decisione della Corte di Giustizia Europea che aveva invalidato lo Scudo Privacy (Privacy Shield), si era formalmente bloccato lo scambio di dati personali tra Europa e Stati Uniti, a causa della mancanza di adeguatezza della normativa statunitense rispetto al GDPR Europeo.

La Commissione Europea, in virtù dei negoziati tra UE e USA durati un paio di anni, dell'ordine esecutivo che Biden aveva firmato nell'ottobre 2022 e dei relativi adeguamenti del Dipartimento di Giustizia statunitense, è giunta alla conclusione che gli **Stati Uniti garantiscono un livello di protezione adeguato comparabile a quello dell'Unione europea**, con protezioni e garanzie sufficienti sul trattamento dei dati personali. Sulla base della nuova decisione di adeguatezza, **i dati personali possono circolare in modo sicuro** dall'UE verso le imprese statunitensi che partecipano al quadro, senza la necessità di ulteriori garanzie per la protezione dei dati.

Il quadro UE-USA per la protezione dei dati personali introduce **nuove garanzie vincolanti** per far fronte a tutte le preoccupazioni espresse dalla Corte di giustizia dell'Unione europea, tra cui la **limitazione dell'accesso ai dati dell'UE da parte dei servizi di intelligence statunitensi** a quanto "necessario e proporzionato" e **l'istituzione di un tribunale del riesame in materia di protezione dei dati (Data Protection Review Court, DPRC)**, accessibile ai cittadini dell'UE. Il nuovo quadro introduce miglioramenti significativi rispetto al meccanismo esistente nell'ambito dello scudo per la privacy.

Le **imprese statunitensi** potranno aderire al quadro UE-USA per la protezione dei dati personali **impegnandosi a rispettare un insieme dettagliato di obblighi in materia di privacy**, ad esempio l'obbligo di cancellare i dati personali quando questi non sono più necessari per lo scopo per il quale sono stati raccolti e di garantire la continuità della protezione quando i dati personali sono condivisi con terzi.

Possiamo così riassumere gli aspetti principali del nuovo accordo UE-USA:

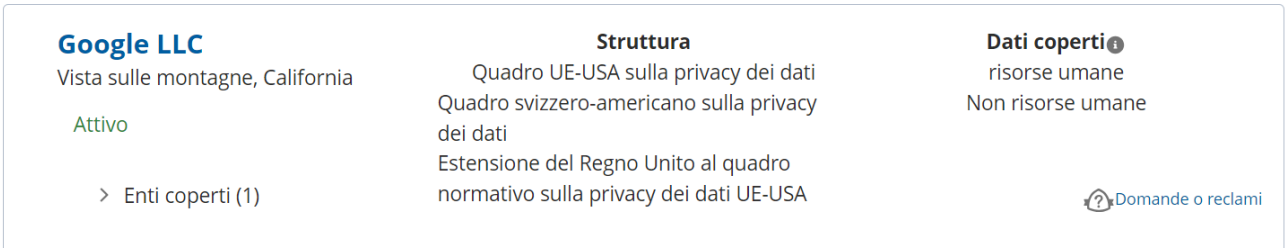
La limitazione dell'accesso ai dati dei cittadini europei da parte dei servizi di intelligence statunitensi a quanto "necessario e proporzionato". Per tutto ciò che riguarda applicazione del diritto penale e sicurezza nazionale, gli Stati Uniti si impegnano a garantire salvaguardie relative all'accesso ai dati trasferiti da parte delle autorità pubbliche statunitensi.

L'istituzione di un tribunale per il riesame della protezione dei dati (Data Protection Review Court, DPRC), "indipendente e imparziale", a cui avranno accesso i cittadini dell'Ue. La Corte indagherà e risolverà autonomamente i reclami, anche adottando misure correttive vincolanti. Qualora questo organismo dovesse rilevare che i dati sono stati raccolti in violazione delle nuove garanzie, potrà ordinarne la cancellazione.

E' garantito l'obbligo di eliminare i dati personali da parte delle società statunitensi che aderiranno a questo nuovo regime di scambio dei dati, quando queste informazioni non sono più necessari per lo scopo per il quale sono stati raccolti. Le stesse aziende si impegnano a garantire la continuità della protezione quando i dati personali sono condivisi con terzi.

Il funzionamento del Data Privacy Framework UE-USA sarà soggetto a revisioni periodiche, che saranno effettuate dalla Commissione europea, insieme ai rappresentanti delle autorità europee per la protezione dei dati e alle autorità statunitensi competenti. Il primo riesame avrà luogo entro un anno dall'entrata in vigore della decisione di adeguatezza, al fine di verificare che tutti gli elementi pertinenti siano stati pienamente recepiti nel quadro giuridico statunitense e funzionino efficacemente nella pratica.

Dall'11 luglio, dunque, i dati personali raccolti in Unione europea ricominciano a essere trasferiti liberamente alle società statunitensi che parteciperanno all'iniziativa, senza bisogno di ulteriori garanzie per la protezione dei dati. I dati potranno quindi essere condivisi solo con quelle aziende che hanno sottoscritto l'accordo. A questo riguardo, è possibile verificare se il fornitore cloud è inserito nella DPF list, cioè l'elenco dei fornitori certificati ai sensi del nuovo accordo. La verifica può essere effettuata accedendo al seguente link https://www.dataprivacyframework.gov/s/participant-search , inserendo nel campo di ricerca il fornitore di cui si vogliono reperire le informazioni di certificazione. Per quanto riguarda Google, è naturalmente presente in elenco:

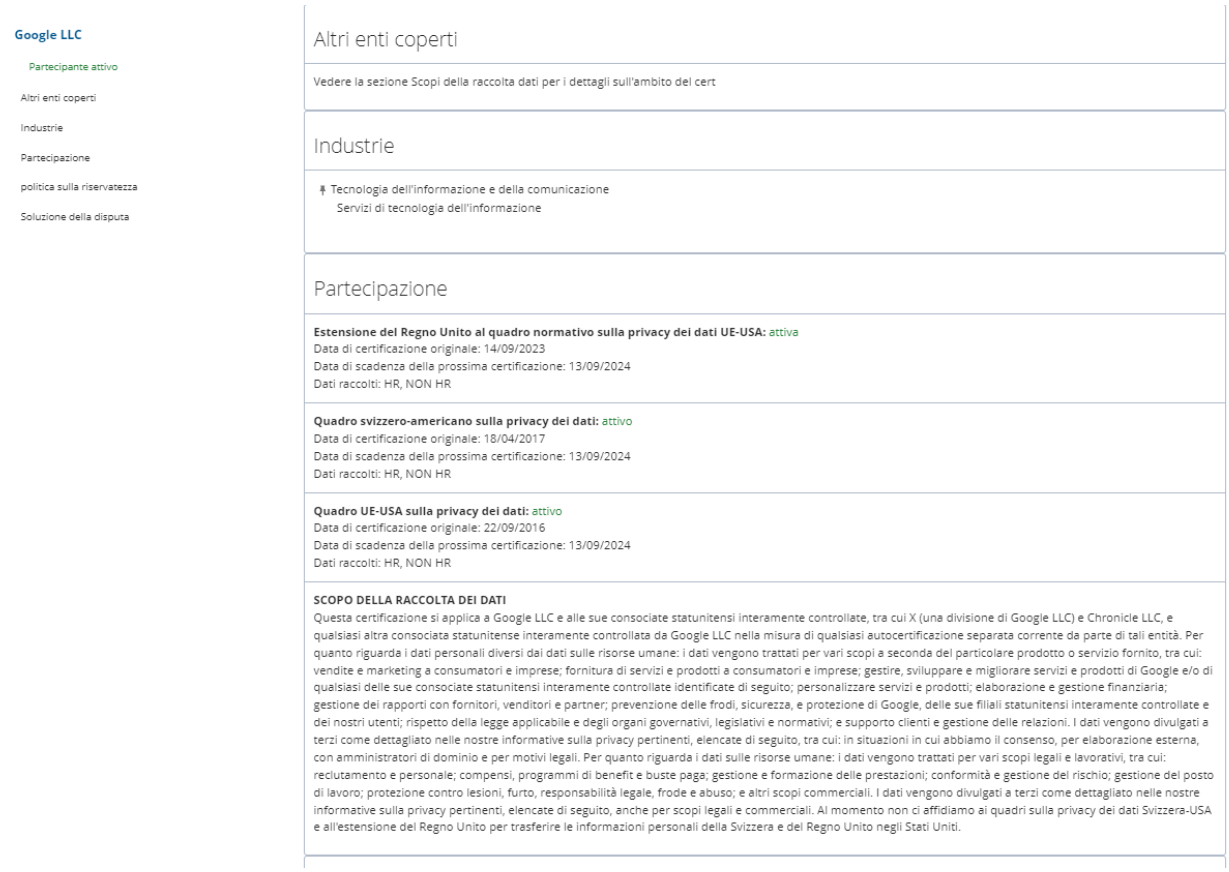



E' facile vedere, infatti, che:

- la certificazione è nello stato Attivo
- le Strutture di dati coperti sono quelle per i trasferimenti UE-USA, Svizzera-America, Regno Unito
- i Dati coperti da certificazione sono quelli Risorse umane (Dati personali relativi ai dipendenti di un'organizzazione, passati o presenti, raccolti nell'ambito del rapporto di lavoro) e Non risorse umane (Altri dati personali).

Entrando poi nel dettaglio del fornitore, è possibile verificare tutta una serie di altri requisiti e informazioni attraverso il menù a disposizione:

**Ref. Dott.ssa Anna CIMA**
Tel. 328.8923614



Google LLC

Partecipante attivo

Altri enti coperti

Industrie

Partecipazione

politica sulla riservatezza

Soluzione della disputa

## Altri enti coperti

Vedere la sezione Scopi della raccolta dati per i dettagli sull'ambito del cert

## Industrie

Tecnologia dell'informazione e della comunicazione
Servizi di tecnologia dell'informazione

## Partecipazione

**Estensione del Regno Unito al quadro normativo sulla privacy dei dati UE-USA:** attiva
Data di certificazione originale: 14/09/2023
Data di scadenza della prossima certificazione: 13/09/2024
Dati raccolti: HR, NON HR

**Quadro svizzero-americano sulla privacy dei dati:** attivo
Data di certificazione originale: 18/04/2017
Data di scadenza della prossima certificazione: 13/09/2024
Dati raccolti: HR, NON HR

**Quadro UE-USA sulla privacy dei dati:** attivo
Data di certificazione originale: 22/09/2016
Data di scadenza della prossima certificazione: 13/09/2024
Dati raccolti: HR, NON HR

**SCOPO DELLA RACCOLTA DEI DATI**
Questa certificazione si applica a Google LLC e alle sue consociate statunitensi interamente controllate, tra cui X (una divisione di Google LLC) e Chronicle LLC, e qualsiasi altra consociata statunitense interamente controllata da Google LLC nella misura di qualsiasi autocertificazione separata corrente da parte di tali entità. Per quanto riguarda i dati personali diversi dai dati sulle risorse umane: i dati vengono trattati per vari scopi a seconda del particolare prodotto o servizio fornito, tra cui: vendite e marketing a consumatori e imprese; fornitura di servizi e prodotti a consumatori e imprese; gestire, sviluppare e migliorare servizi e prodotti di Google e/o di qualsiasi delle sue consociate statunitensi interamente controllate identificate di seguito; personalizzare servizi e prodotti; elaborazione e gestione finanziaria; gestione dei rapporti con fornitori, venditori e partner; prevenzione delle frodi, sicurezza, e protezione di Google, delle sue filiali statunitensi interamente controllate e dei nostri utenti; rispetto della legge applicabile e degli organi governativi, legislativi e normativi; e supporto clienti e gestione delle relazioni. I dati vengono divulgati a terzi come dettagliato nelle nostre informative sulla privacy pertinenti, elencate di seguito, tra cui: in situazioni in cui abbiamo il consenso, per elaborazione esterna, con amministratori di dominio e per motivi legali. Per quanto riguarda i dati sulle risorse umane: i dati vengono trattati per vari scopi legali e lavorativi, tra cui: reclutamento e personale; compensi, programmi di benefit e buste paga; gestione e formazione delle prestazioni; conformità e gestione del rischio; gestione del posto di lavoro; protezione contro lesioni, furto, responsabilità legale, frode e abuso; e altri scopi commerciali. I dati vengono divulgati a terzi come dettagliato nelle nostre informative sulla privacy pertinenti, elencate di seguito, anche per scopi legali e commerciali. Al momento non ci affidiamo ai quadri sulla privacy dei dati Svizzera-USA e all'estensione del Regno Unito per trasferire le informazioni personali della Svizzera e del Regno Unito negli Stati Uniti.

Alla luce di questo quadro, **è quindi possibile riattivare tutte le funzionalità della piattaforma digitale che la scuola ha in uso** (es. Google Workspace, Microsoft, ecc…) e che aveva sospeso.

Per questo motivo, ho aggiornato la **base documentale**, che dovrà essere **personalizzata e acquisita agli atti** da tutte quelle scuole che hanno in uso **la piattaforma cloud**. Si precisa che i documenti rappresentano appunto una **base**, costruiti su processi standard e considerando una minimizzazione dei dati e dei servizi tramite la piattaforma. Ogni scuola ha però il compito di verificare se l'impostazione è rispondente alla propria organizzazione e ha l'onere di adeguare i documenti ai propri processi.

Segue l'elenco degli allegati ed una breve descrizione, specificando che sono impostati per la piattaforma **Google Workspace**. Chi utilizza Microsoft o altre piattaforme dovrà personalizzarli:

1) Registro dei Trattamenti
2) DPIA per l'utilizzo della piattaforma cloud Google Workspace
3) Incarico interno Amministratore piattaforma
4) Informativa privacy per l'utilizzo della piattaforma cloud
5) Disciplinare studenti per il corretto utilizzo della piattaforma cloud
6) Regolamento per il personale per il corretto utilizzo della piattaforma cloud
7) Gestione violazione dati (Data Breach)
8) Registro delle violazioni (Data Breach)

Si consiglia di creare un fascicolo digitale in cui raccogliere tutta la documentazione.

## 1. REGISTRO DEI TRATTAMENTI

E' l'insieme dei tipi di trattamenti effettuati dalla scuola, in cui sono specificati le categorie di interessati, i tipi di dati, gli strumenti del trattamento, le modalità del trattamento e ogni altra informazione correlata. E' stato aggiornato rispetto alla versione precedente e ciascuna scuola dovrà effettuare le **seguenti personalizzazioni**:

- Sul primo foglio (Informazioni e contatti) inserire i **dati della scuola** e la **data di compilazione/aggiornamento**
- Sul quarto foglio (Responsabili del Trattamento) inserire i **fornitori nominati come Responsabili esterni** (vedere nota rossa all'interno)

Il Registro va tenuto agli atti e **NON** è soggetto a pubblicazione.

## 2. DPIA PER L'UTILIZZO DELLA PIATTAFORMA

Il GDPR prevede che, quando il trattamento può comportare un **rischio elevato per i diritti e le libertà delle persone**, è necessario effettuare la **Valutazione d'Impatto sulla Protezione dei Dati (DPIA).** Attraverso questo documento la scuola, in riferimento al trattamento effettuato, ne valuta la necessità, la proporzionalità e i relativi rischi, decidendo poi se intraprendere/continuare il trattamento o sospenderlo.

Ciascuna scuola dovrà effettuare le **seguenti personalizzazioni:**

- Sulla pag.1 inserire i **dati della scuola** e il **nome DS**
- Sull'ultima pag. inserire **il nome DS**

Il documento va tenuto agli atti e **NON** è soggetto a pubblicazione.

*Nota: la TIA che era stata precedentemente elaborata non è più necessaria, perché il trasferimento dati ad aziende statunitensi è stato ritenuto adeguato tramite il nuovo Accordo.

## 3. INCARICO INTERNO AMMINISTRATORE DELLA PIATTAFORMA

Tra le misure tecniche e organizzative adottate dal Titolare, c'è la nomina di un amministratore della piattaforma, che abbia le conoscenze e l'esperienza per poter efficacemente gestire la console.

Ciascuna scuola dovrà effettuare le **seguenti personalizzazioni:**

- Sulla pag.1 inserire i **dati di protocollazione** (o eliminare se si aggiunge la stampa del protocollo digitale) i **dati della scuola,** il **nome DS** e i **dati del soggetto incaricato**
- Sulla pag.2 inserire il **nome DS**, il **nome Incaricato**, le **firme**

La nomina deve quindi essere regolarizzata tra le parti e tenuta agli atti.

## 4. INFORMATIVA PRIVACY

Il GDPR (artt. 13-14) prevede che per ogni trattamento dati effettuato, il Titolare debba informare gli Interessati, fornendo tutte le informazioni necessarie a valutare la gestione dei propri dati (finalità, basi giuridiche, modalità, tipologia di dati, trasferimento dati, …).

Questo specifico trattamento non prevede il consenso degli interessati interni, perché la scuola agisce per finalità istituzionali e per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

Ciascuna scuola dovrà effettuare le **seguenti personalizzazioni:**

- Sulla pag.1 inserire i **dati della scuola**

L'Informativa **DEVE** essere pubblicata nella sezione privacy del sito web e **notificata** a tutti gli interessati (docenti, alunni, famiglie) tramite le **comunicazioni del Registro elettronico** e con **spunta di presa visione**.

## 5. DISCIPLINARE PER STUDENTI

Dopo aver valutato l'utilizzo della piattaforma, la scuola deve fornire indicazioni sul corretto utilizzo della stessa a tutti gli utenti, e gli alunni sono sicuramente (per età e indole) quelli più bisognosi di chiare regole. Il Disciplinare spiega i principi, l'organizzazione e definisce le norme di comportamento da seguire nell'uso della piattaforma cloud. In relazione all'età, è opportuno che anche le famiglie ne prendano visione.
Ciascuna scuola dovrà effettuare le **seguenti personalizzazioni:**

- Inserire l' **intestazione della scuola**
- Sulla pag.5 inserire **il nome DS**

Il Disciplinare **DEVE** essere **notificato** a tutti gli alunni tramite le **comunicazioni del Registro elettronico** e con **spunta di presa visione**. NON è necessaria la pubblicazione perché contiene misure tecniche e organizzative interne non soggette a diffusione.

## 6. REGOLAMENTO PER DOCENTI

Anche per il personale è necessario che la scuola fornisca le opportune indicazioni sul corretto utilizzo della piattaforma, fornendo informazioni sugli aspetti tecnici/organizzativi e sul trattamento dati.
Ciascuna scuola dovrà effettuare le **seguenti personalizzazioni:**

- Inserire l' **intestazione della scuola**
- Sulla pag.11 inserire **il nome DS**

Il Regolamento **DEVE** essere **notificato** a tutti i Docenti tramite le **comunicazioni del Registro elettronico** e con **spunta di presa visione**. NON è necessaria la pubblicazione perché contiene misure tecniche e organizzative interne non soggette a diffusione.

## 7. GESTIONE VIOLAZIONE DATI (DATA BREACH)

L'uso delle nuove tecnologie e di ambienti digitali, espone qualunque titolare del trattamento al rischio di una violazione dati, che può essere più o meno probabile in relazione alle misure tecniche e organizzative adottate e al livello di attenzione e responsabilità degli utenti nell'uso di tali strumenti. Le cause della violazione possono essere accidentali/colpose, senza quindi alcuna volontà del fatto, oppure dolose (es. hacker o terzi non autorizzati), che volontariamente attuano azioni che mettono a rischio i dati e quindi rappresentino un rischio per i diritti e le libertà delle persone fisiche. Diversi possono anche essere gli effetti dell'evento, ed è quindi necessario spiegare agli utilizzatori come devono agire nel caso dovessero riscontrare eventi potenzialmente rischiosi. Tutto questo è spiegato nel Documento di gestione della violazione dati (Data Breach).
Ciascuna scuola dovrà effettuare le **seguenti personalizzazioni:**

- Inserire l' **intestazione della scuola**
- Sulla pag.6 inserire **il nome DS**

Il Documento Data Breach **DEVE** essere **notificato** a tutti gli interessati (docenti, alunni, famiglie) tramite le **comunicazioni del Registro elettronico** e con **spunta di presa visione**. NON è soggetto a pubblicazione.

## 8. REGISTRO VIOLAZIONE DATI (DATA BREACH)

Il Titolare del trattamento *deve documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio* (art.33 GDPR). A tal proposito, ho predisposto un Registro delle violazioni.
Ciascuna scuola dovrà effettuare le **seguenti personalizzazioni:**

- Inserire i **dati della scuola**

Il documento va tenuto agli atti e **NON** è soggetto a pubblicazione.

## 9. RIEPILOGO DOCUMENTI

| | DOCUMENTO | PERSONALIZZAZIONE | NOTE |
|---|---|---|---|
| **1** | **REGISTRO DEI TRATTAMENTI** | Foglio 1: dati scuola e data<br>Foglio 4: vedere nota rossa | -Tenere agli atti<br>-NON pubblicare |
| **2** | **DPIA** | Pag.1: dati scuola e nome DS<br>Pag. ultima: nome DS | -Tenere agli atti<br>-NON pubblicare |
| **3** | **Incarico Amministratore** | Pag. 1: Dati della scuola, nome DS, nome Incaricato<br>Pag. 2: nome DS, nome Incaricato, firme | -Tenere agli atti<br>-NON pubblicare |
| **4** | **Informativa privacy** | Pag.1: dati della scuola | -Tenere agli atti<br>-Pubblicazione sito sez. privacy<br>-Notifica agli interessati tramite RE |
| **5** | **Disciplinare per studenti** | Pag. 1: intestazione scuola<br>Pag. 5: nome DS | -Tenere agli atti<br>-Notifica agli interessati tramite RE<br>-NON pubblicare |
| **6** | **Regolamento per docenti** | Pag. 1: intestazione scuola<br>Pag. 11: nome DS | -Tenere agli atti<br>-Notifica agli interessati tramite RE<br>-NON pubblicare |
| **7** | **Gestione violazione dati** | Pag. 1: intestazione scuola<br>Pag. 6: nome DS | -Tenere agli atti<br>-Notifica agli interessati tramite RE<br>-NON pubblicare |
| **8** | **Registro delle violazioni** | Singolo foglio: dati della scuola | -Tenere agli atti<br>-NON pubblicare |

Tutti i documenti devono essere eventualmente adeguati ai propri specifici processi e alla propria gestione della piattaforma, essere protocollati e firmati, gestiti come indicato nelle note e conservati in un fascicolo digitale in modo da essere facilmente reperibili.

Si consiglia di diramare una circolare rivolta a tutti gli utenti della scuola (personale, alunni, famiglie) raccomandando di prendere visione dei documenti che saranno loro notificati.

---

Con specifico riguardo alla piattaforma Google Workspace, si raccomanda di:

1) Verificare la **sottoscrizione del contratto di Workspace**, accedendo alla console come super amministratore > Account > Impostazioni account > Aspetti legali e conformità, e chi non l'avesse ancora fatto deve accettare *l'Addendum per il trattamento dei dati Cloud (CDPA)*
2) Attivare solo i **servizi principali** messi a disposizione da Google, escludendo quelli aggiuntivi se non sono strettamente necessari. Per questi ulteriori servizi aggiuntivi, la scuola deve chiedere esplicito consenso alle famiglie (o alunni in caso di maggiorenni).

Resto a disposizione per eventuali chiarimenti.

Data 02/10/2023

Cordiali Saluti
Dott.ssa Anna CIMA