Da: drsi.staff@istruzione.it
Oggetto: Supporto tecnico alla valutazione di conformità al GDPR del trattamento e trasferimento extra UE di dati personali degli utenti delle Istituzioni scolastiche attraverso determinati servizi PEO e piattaforme ICT
Data: 29/03/2023 08:41:27

Si trasmette la nota n. 14280 del 29 marzo 2023.
Cordiali saluti.

Ufficio di diretta collaborazione del Direttore Generale
Ministero dell'istruzione e del merito
Ufficio Scolastico Regionale per la Sicilia

https://www.usr.sicilia.it/

Ministero dell'istruzione e del merito

Ufficio Scolastico Regionale per la Sicilia

Ufficio di diretta collaborazione del Direttore Generale

Ai Dirigenti delle Istituzioni scolastiche
della Sicilia

e, p.c. Ai Dirigenti degli Ambiti Territoriali
dell'USR Sicilia

Oggetto: Supporto tecnico alla valutazione di conformità al GDPR del trattamento e trasferimento extra UE di dati personali degli utenti delle Istituzioni scolastiche attraverso determinati servizi PEO e piattaforme ICT.

Il Ministero ha ritenuto di formulare degli approfondimenti tecnici e fornire misure specifiche, che si allegano alla presente, per far fronte alle criticità sulla valutazione di conformità al GDPR del trattamento e trasferimento transfrontaliero verso Paesi terzi (in particolare, tra gli altri, gli Stati Uniti) di dati personali degli utenti delle Istituzioni Scolastiche Autonome e dei loro corrispondenti mediante determinati servizi PEO e piattaforme ICT.

Si invitano le SS.LL. a prenderne visione, coinvolgendo i propri referenti informatici, i DPO, nonché i fornitori dei servizi ICT delle Scuole.

Il Direttore Generale
Giuseppe Pierro

Firmato digitalmente da
PIERRO GIUSEPPE
C=IT
O=MINISTERO DELL'ISTRUZIONE

Via Giovanni Fattori n° 60 – 90146 Palermo - Tel. 091/6909111
E-mail: direzione-sicilia@istruzione.it - PEC: drsi@postacert.istruzione.it - www.usr.sicilia.it

Ministero dell'istruzione e del merito

Dipartimento per le risorse umane, finanziarie e strumentali
Direzione generale per i sistemi informativi e la statistica

APPROFONDIMENTI TECNICI DI SUPPORTO PER LE ISTITUZIONI SCOLASTICHE

Sulla base del principio di accountability (responsabilizzazione) previsto dal Regolamento UE 2016/679 (GDPR), i titolari del trattamento sono tenuti a condurre un'analisi del rischio o valutazione d'impatto ed una verifica di adeguatezza circa le modalità, le garanzie ed i limiti del trattamento dei dati personali nel rispetto della normativa vigente. A tale fine lo European Data Protection Board (EDPB) raccomanda che il titolare conservi la documentazione utile a ricostruire le valutazioni condotte al fine di rendicontare quanto svolto di fronte all'Autorità Garante, ove richiesto.

Considerato l'ambito di applicazione territoriale del GDPR, che ai sensi dell'art. 3 del citato Regolamento si estende anche ai trattamenti di dati personali dei residenti UE effettuati fuori dallo Spazio Economico Europeo, preme sottolineare l'importanza di verificare il luogo di stabilimento del fornitore di servizi ICT e l'ubicazione dei data center coinvolti nel trattamento ai fini di valutare l'applicabilità o meno delle garanzie previste per il trasferimento dei dati personali verso paesi terzi. (Capo V articoli 44 e seguenti del GDPR).

In merito alla questione del trasferimento dei dati tra Europa e Stati Uniti, preme ricordare quanto segue:

- La Corte di Giustizia dell'Unione Europea (CGUE) nel caso C 311/18, meglio noto come "Schrems II" ha dichiarato l'invalidità della decisione di adeguatezza n. 1250 del 2016 ("Privacy Shield") con la quale l'Unione Europea aveva validato il contenuto della normativa sul trasferimento dei dati, autorizzando il flusso transfrontaliero tra i Paesi membri dell'Unione Europea e gli Stati Uniti, sulla base del meccanismo previsto dall'art. 45 GDPR.
- In mancanza di una nuova decisione di adeguatezza che consenta il trasferimento ai sensi dell'articolo 45 citato, il titolare del trattamento o il responsabile del trattamento può comunque trasferire dati personali verso gli Stati Uniti, solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Possono costituire garanzie adeguate le misure indicate all'art. 46 del GDPR.
- La CGUE nella sopra menzionata decisione "*Schrems II*" ha precisato che ogni titolare del trattamento è responsabile delle verifiche, caso per caso, dei singoli flussi transfrontalieri dei dati, le cui misure di

Direttore Generale
Ing. Davide D'Amico

PEC: dgsis@postacert.istruzione.it
e-*mail:* dgsis.segreteria@istruzione.it

Tel 06 5849 – 4001 – 4002 - 4003

sicurezza devono essere valutate in base alle caratteristiche del trattamento e alle finalità del trasferimento.

- Pertanto, si invita a verificare che i servizi ICT in uso siano conformi al "*GDPR*" attraverso i relativi accordi di servizio, che costituiscono base giuridica del trattamento ai sensi dell'art. 28 del GDPR. In particolare, si invita a verificare se tali accordi di servizio prevedono ed autorizzano trasferimenti internazionali dei dati e se questi **avvengono sulla base delle garanzie indicate all'art. 46 del GDPR**.

Relativamente a Microsoft e Google al fine di agevolare la verifica di conformità del trattamento dei dati personali al GDPR, che le istituzioni scolastiche hanno la responsabilità di condurre in qualità di titolari del trattamento, si segnalano alcuni documenti utili ad una prima valutazione (che andrà poi verificata secondo lo specifico contratto sottoscritto e dei dati trattati). Stante il carattere tecnico della seguente documentazione, è importante invitare le istituzioni scolastiche a prenderne visione coinvolgendo i propri referenti informatici e i DPO, eventualmente supportati dai fornitori dei servizi ICT delle scuole.

Appare innanzitutto opportuno evidenziare, che tanto Microsoft quanto Google, nella documentazione ufficiale caricata sui rispettivi siti internet dichiarino che il trattamento dei dati, ivi incluso gli aspetti dei trasferimenti transfrontalieri degli stessi, risulti essere *conforme* rispetto alle norme del GDPR.

Specificatamente, dette affermazioni sono reperibili tra l'altro:

- **per MICROSOFT**

Nel documento Data Processing Agreement (DPA) nella versione aggiornata del 1 Gennaio 2023 dove viene precisato che:

<<Tutti i trasferimenti dei Dati Personali fuori dall'Unione Europea effettuati da Microsoft per fornire i Prodotti e i Servizi, verranno disciplinati dalle Clausole Contrattuali Tipo 2021 adottate da Microsoft. Tutti i trasferimenti di Dati Personali verso un paese terzo o un'organizzazione internazionale saranno soggetti alle misure di sicurezza appropriate descritte nell'Articolo 46 del GDPR e tali trasferimenti e misure di sicurezza saranno documentati conformemente all'Articolo 30(2) del GDPR>> (cfr. pagina 9 -trasferimento dei dati);

<<Per quanto riguarda i Servizi Online, ai quali viene applicata la soluzione EU Data Boundary, Microsoft archivierà e tratterà i Dati della Società all'interno dell'Unione Europea come stabilito nelle Condizioni per l'Utilizzo dei Prodotti>> (cfr. pag.10 - Posizione dei Dati della Società).

Riguardo al secondo punto, appare opportuno verificare che i servizi utilizzati non siano tra quelli temporaneamente o permanentemente esclusi (link). Particolare attenzione si ponga sulla versione di Office 365 utilizzata, posto che per le *<<Applicazioni Microsoft 365 (per build precedenti al 31 dicembre 2022): per garantire prestazioni e stabilità ai clienti esistenti che usano applicazioni Microsoft 365, gli impegni relativi ai limiti dei dati dell'UE si applicano solo alle versioni rilasciate dopo il 31 dicembre 2022. I clienti che usano build precedenti devono eseguire l'aggiornamento alla versione più recente>>*

- **per GOOGLE**

La società effettua il trattamento dei dati personali dei clienti dei servizi Google Cloud Platform, Google Workspace e Cloud Identity sulla base del Cloud Data Processing Addendum (CDPA). Il suddetto CDPA disciplina i trasferimenti internazionali di dati all'articolo 10, specificando che in caso il trasferimento avvenga verso un paese non coperto da una decisione di adeguatezza, allo stesso si applicano gli SCC, clausole contrattuali tipo, previste dall'articolo 46 GDPR (*<<if Google's address is not in an Adequate Country, the SCCs (Controller-to-Processor) and/or SCCs (Processor-to-Processor) will apply (according to whether Customer is a controller and/or processor) with respect to such Restricted European Transfers between Google and Customer.>>*).

Detta informazione è altresì reperibile nelle stesse pagine informative dedicate alla privacy nel rispetto del GDPR.

Inoltre è importante condividere i seguenti passaggi pubblicati ed i relativi riferimenti:

<<Google Workspace for Education può essere utilizzato in conformità con il GDPR. Il nostro Emendamento sul trattamento dei dati è progettato per soddisfare i requisiti di adeguatezza e sicurezza del GDPR; inoltre, la Commissione europea ha creato delle clausole contrattuali tipo per consentire in particolare il trasferimento dei dati personali dall'Europa. I clienti possono aderire all'Emendamento sul trattamento dei dati e alle clausole contrattuali tipo.>> (Domande frequenti sulla privacy e sulla sicurezza)

<<Nel caso in cui i dati personali vengano trasferiti fuori dall'UE in paesi terzi non coperti da decisioni di adeguatezza, ci impegniamo a fronte dei nostri contratti per il trattamento dei dati a mantenere un meccanismo che faciliti questi trasferimenti secondo quanto stabilito dal GDPR.>> (Trasferimento internazionale dei dati).

Si noti che a seconda degli ulteriori servizi eventualmente previsti nel contratto, le misure possono essere ulteriormente rafforzate prevedendo anche forme di mitigazione del rischio attraverso la pseudoanonimizzazione e la cifratura dei dati lato client: (Configurare il servizio chiavi per la crittografia lato client) .

Inoltre, si coglie l'occasione di ricordare che le misure del PNRR 1.2 - Migrazione al cloud (cloud qualificati) e 1.4.1 – siti web delle scuole, a cui la stragrande maggioranza delle istituzioni scolastiche ha aderito, possono rappresentare strumenti finalizzati anche a preservare l'utilizzo dei dati personali e sensibili del personale e degli alunni, utilizzando per comunicazioni di particolari tipologie di dati, servizi implementati su cloud qualificati e su aree ad accesso riservato dei siti web delle scuole.

IL DIRETTORE GENERALE

Ing. Davide D'Amico

Direttore Generale
Ing. Davide D'Amico

PEC: dgsis@postacert.istruzione.it
e-*mail:* dgsis.segreteria@istruzione.it

Tel 06 5849 – 4001 – 4002 - 4003