Informazioni sulla DPIA

Nome della PIA
Microsoft Office 365

Nome autore
DPO Esempio Antonio

Nome validatore
DPO Esempio Antonio

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?
Il Trattamento preso in considerazione è quello offerto dai servizi di Microsoft 365, in relazione al passaggio di dati che avviene tra i Paesi Membri dell'Unione Europea e gli Stati Uniti.

Quali sono le responsabilità connesse al trattamento?
L'istituto scolastico è il Titolare del Trattamento e il Dirigente scolastico in quanto responsabile legale ha il compito di rispettare le norme vigenti del GDPR in materia di protezione dei dati e dei trasferimenti degli stessi verso i Paesi al di fuori dell'Unione Europea.
Microsoft è Responsabile esterno al Trattamento dati essendo il provider dei servizi informatici utilizzati all'interno dell'Istituto scolastico, il servizio reso da Microsoft deve presentare garanzie che mettano in atto misure tecniche e organizzative adeguate per rispettare i requisiti preposti del GDPR e allo stesso tempo deve garantire la tutela dei Diritti degli interessati.

Cosa afferma Microsoft in merito al trattamento?
Nel documento **Data Processing Agreement** (DPA) di Microsoft nella versione aggiornata del 1 Gennaio *2023 si legge:*

<<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).

Quali servizi Microsoft in merito al trattamento l'Istituto scolastico non utilizza?
L'Istituto scolastico **non utilizza** tutti quei servizi temporaneamente o permanentemente esclusi disponibili al seguente URL: https://learn.microsoft.com/it-it/privacy/eudb/eu-data-boundary-permanent-transfers-from-services

Ci sono standard applicabili al trattamento?

Gli Standard definiti per il problema in esame fanno riferimento alla verifica sui singoli flussi di dati, in particolare che tali dati siano trasferiti secondo gli standard di adeguatezza come previsto dal GDPR. Il DPO deve verificare che i servizi ICT in uso siano conformi al GDPR attraverso i relativi accordi di servizio.

Versione di Office 365 conforme e applicabile al trattamento?

L'Istituto scolastico utilizza, alla data del presente documento, la versione 2023 - 11 aprile, Versione 2303 (Build 16227.20280) Microsoft ricorda: *<<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>>*

Valutazione: Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati oggetto di trasferimento transfrontaliero sono l'indirizzo IP del dispositivo dell'utente e le informazioni relative al browser, al sistema operativo, alla risoluzione dello schermo, alla lingua selezionata e alla data e ora della visita al sito web, questi dati raccolti e trasferiti sono conservati per un tempo di 18 mesi. I soggetti che possono accedere a questi dati sono i dipendenti di MICROSOFT OFFICE 365, le società consociate o le società che agiscono per conto di MICROSOFT OFFICE 365, sono tutti vincolati ai termini di riservatezza e opportunamente incaricati al trattamento ai sensi dell'art. 28,c del Regolamento Europeo 679/2016 (*data verifica DPO, 31/03/2023)*

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Il ciclo di vita passa attraverso una serie di fasi: si va dalla raccolta di dati personali, alla manipolazione durante la fase di espletamento e dell'utilizzo dei servizi offerti, alla conservazione e all'archiviazione, fino alla distruzione degli stessi dopo 18 mesi.

Quali sono le risorse di supporto ai dati?

Le risorse che ospitano le informazioni sono le varie strumentazioni informatiche utilizzate che possono essere tablet, pc, smatphone, che sono basati su diversi sistemi operativi che permettono la fruizione dei servizi offerti da Microsoft.

Valutazione: Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Si ritiene che il Trattamento sia svolto nell'interesse pubblico ovvero per poter svolgere l'attività di formazione e istruzione nei confronti degli studenti, diritto sancito a livello Costituzionale ex art.34.
Inoltre il Trattamento su strumenti CLOUD è altamente consigliato perché più sicuro rispetto all'uso tradizionale.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Le basi legali che rendono lecito il trattamento sono:
- La Costituzione nell'art.34 sancisce il diritto all'istruzione.
- I contratti stipulati tra il Titolare del trattamento (le istituzioni scolastiche) e i Responsabili del trattamento (Microsoft), ovvero rispettivamente *Cloud Data Processing Addendum CDPA* e *Data Processing Agreement DPA;* all'interno di questi sono presenti clausole che autorizzano la legittimità del Trattamento posto in essere.

Microsoft Office 365 è un servizio SaaS qualificato dall'Agenzia Italiana per la Cybersicurezza Nazionale (ACN), la scheda di servizio qualificato è disponibile al seguente URL: https://catalogocloud.acn.gov.it/service/90

Nella scheda del servizio qualificato si legge:

Il prodotto Office365/Microsoft365 è un servizio basato su cloud studiato per rispondere alle esigenze di sicurezza, affidabilità e produttività delle organizzazioni. Esso combina le applicazioni Office per desktop e dispositivi mobili con le versioni Cloud degli strumenti di comunicazione e collaborazione (Word, Excel, PowerPoint, OneNote, Outlook/Exchange, SharePoint, OneDrive, Stream, Teams, Access, Project, Planner, PowerApps, Power Automate, Visio, Yammer, Defender, Viva) per favorire la produttività degli utenti ovunque si trovino. Per rispondere alle diverse necessità delle singole Amministrazioni, Office365/Microsoft365 è configurabile in base alle funzionalità e alla scalabilità richieste. Esistono diverse tipologie di supporto tecnico remoto e/o on site (a pagamento).

Valutazione: Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati raccolti sono necessari al trattamento in quanto si parla di dati che permettono la connessione e l'utilizzo delle tecnologie e dei servizi che rendono l'Istruzione digitalizzata, in un Mondo che va sempre più verso questa direzione.

Microsoft nel rispetto dei principi di minimizzazione e conservazione del dato digitale opera la cifratura AES del dato archiviato sui servizi. Gli standard e le certificazioni di Microsoft sono le seguenti:

CIS Benchmark CSA-STAR-Self-Assessment ISO 27001 ISO 27017 ISO 27018 SOC 1 SOC 2 FDA CFR Title 21 Part 11 FedRAMP FERPA FIPS 140-2 NIST Cybersecurity Framework (CSF) FFIEC FISC (Japan) GLBA GxP HIPAA/HITECH HITRUST NEN-7510 (Netherlands) SOX BIR 2012 (Netherlands) CCSL/IRAP (Australia) CS Gold Mark (Japan) EN 301 549 (EU) ENISA IAF (EU) ENS (Spain) EU-Model-Clauses EU-U.S. Privacy Shield GDPR (EU) MTCS (Singapore) My Number (Japan) NZ CC Framework (New Zealand) PDPA (Argentina) PIPEDA (Canada) UK-G-Cloud

Microsoft è in possesso della certificazione ISO/IEC 27001 estesa con i controlli degli standard ISO/IEC 27017 e ISO/IEC 27018 disponibile al seguente link
https://catalogocloud.acn.gov.it/serve/90/docs/e4e58e5bc8b8734c045d865b0fffbde74a0059e8b4f36e0d4afeb343b1d6ebfb/O365%20ISO%2027001%20CON%20STATEMENT%20%2027017%2027018.pdf

Valutazione: Accettabile

I dati sono esatti e aggiornati?

Le misure previste per garantire la qualità dei dati sono quelle previste all'interno dei contratti stipulati, CDPA e DPA.

CDPA: https://learn.microsoft.com/it-it/microsoft-365/compliance/compliance-manager-templates-list?view=o365-worldwide

DPA: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?

Tutti i dati conservati da Microsoft nei servizi Cloud storage sono resi anonimi, minimizzati e cifrati. Inoltre sono evirati parzialmente dell'indirizzo IP (dopo 9 mesi) e delle informazioni sui cookie (dopo 18 mesi).
Dopo 18 mesi sono cancellati come previsto dalla normativa europea.

Valutazione: Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati sono informati tramite apposite informative connesse al consenso e qualora i dati dovessero essere utilizzati per uno scopo non contemplato nelle norme riferite alla privacy si richiede un ulteriore consenso. Nella sezione Controllo privacy si ha l'opportunità di esaminare e modificare tutte le informazioni riguardanti la privacy.
Ogni utente è libero di personalizzare il proprio account in termini di privacy, l'amministratore di sistema, opportunamente designato, applica periodicamente controlli e aggiornamenti globali alla piattaforma, tali aggiornamenti di sicurezza si applicano verticalmente a tutti gli utenti.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Il Consenso si ottiene attraverso l'accettazione delle varie clausole ponendo una spunta in fase di registrazione.
Per gli studenti il consenso è richiesto in fase di rilascio dell'account. E' espresso dai tutori legali per gli studenti minorenni.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Gli interessati possono rivolgersi direttamente all'amministratore designato dall'Istituto per l'esercizio dei loro diritti.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Gli interessati possono rivolgersi direttamente all'amministratore designato dall'Istituto per l'esercizio dei loro diritti.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Gli interessati possono rivolgersi direttamente all'amministratore designato dall'Istituto per l'esercizio dei loro diritti.

Valutazione: Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

I Responsabili del trattamento sono legati al Titolare da un contratto che viene accettato e all'interno dello stesso sono descritti gli ambiti di responsabilità e gli obblighi specifici con relative incombenze.

Valutazione: Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

In caso di trasferimento verso Paesi Esteri secondo la nota Ministeriale n. 0000706 del 20.03.2023, i dati possono essere trasferiti ai sensi dell'art. 45 del GDPR solo se si forniscono garanzie adeguate e a condizione che gli interessati dispongano dei diritti azionabili e di mezzi di ricorso effettivi (misure adeguate ex art.46 GDPR); quindi alla stipula contrattuale il Titolare del trattamento e il Responsabile del trattamento adeguano i contratti rispetto alla normativa prevista dal GDPR in modo tale da offrire tutela anche per il trasferimento dati verso Paesi fuori dall'Unione Europea.

Il regolamento generale sulla protezione dei dati dell'Unione europea (UE) regola il trasferimento dei dati personali dei clienti UE verso paesi al di fuori dell'Area Economica Europea (AEE) che include tutti i paesi dell'Unione Europea, Islanda, Liechtenstein e Norvegia. A livello pratico, la conformità alle leggi sulla protezione dei dati dell'UE significa anche che i clienti hanno bisogno di meno approvazioni da parte delle singole autorità per trasferire i dati personali al di fuori dell'UE, poiché la maggior parte degli Stati membri dell'UE non richiede un'autorizzazione aggiuntiva se il trasferimento è basato su un accordo conforme alle clausole modello.

Il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea (UE) regola il trasferimento dei dati personali dei clienti in paesi al di fuori dell'Area Economica Europea (AEE), che include tutti i paesi dell'Unione europea, Islanda, Liechtenstein e Norvegia. Microsoft offre ai clienti le clausole contrattuali standard dell'Unione Europea che forniscono garanzie specifiche sui trasferimenti di dati personali per i servizi nell'ambito. Le clausole contrattuali standard dell'Unione Europea vengono utilizzate negli accordi tra provider di servizi (come Microsoft) e i loro clienti per garantire che tutti i dati personali che lasciano l'Area Economica Europea vengano trasferiti in conformità con il GDPR.

Nel luglio 2020, la Corte di giustizia dell'Unione europea (CGUE) ha reso non valido il Privacy Shield UE-USA per i trasferimenti di dati personali dall'UE agli Stati Uniti. Tuttavia, le clausole contrattuali standard dell'Unione Europea continuano a fornire un meccanismo valido per il trasferimento dei dati personali dall'UE e dall'Area Economica Europea, nonché dalla Svizzera e dal Regno Unito. Microsoft rende disponibili le clausole contrattuali standard dell'Unione Europea ai clienti come descritto nelle Condizioni di Microsoft Online Services (OST) Data Protection Addendum (DPA).

Fonte: https://learn.microsoft.com/it-it/compliance/regulatory/offering-eu-model-clauses

Valutazione: Accettabile

Rischi

Misure esistenti o pianificate

Crittografia

I dati sono trattati tramite l'utilizzo di meccanismi di conservazione e comunicazioni cifrati, ai fini di garantire la minimizzazione del rischio di accesso agli stessi.
L'amministratore di sistema opportunamente designato dall'Istituto scolastico è in grado di accedere a tali prospetti, non può accedere alle informazioni, ma può verificare che i dati siano integri e opportunamente protetti.

Valutazione: Accettabile

Anonimizzazione

Gli indirizzi IP (dato particolare oggetto di trasferimento) sono in anonimizzati così da garantire il diritto alla riservatezza e il rispetto del principio di minimizzazione dei dati.

Valutazione: Accettabile

Accesso illegittimo ai dati - RISCHIO

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Diffusione di dati personali di minori, concernenti le attrezzature utilizzate dagli stessi (device) per l'utilizzo dei servizi offerti dai responsabili del Trattamento.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Negazione del diritto all'oblio, rischio arginabile in quanto è possibile presentare ricorso all'autorità di garanzia europea e statunitense.

Quali sono le fonti di rischio?

La fonte di rischio risiede nello stesso trasferimento dati, i dati trasferiti sono dati di tipo particolare.
rischio arginabile in quanto l'impatto sulla sfera privata dell'interessato è minimo. Le informazioni riguardano i device utilizzati e pertanto il dato oggetto di rischio è minimo.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Anonimizzazione, VPN, Firewall.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile, Il rischio è da ritenere trascurabile in quanto i dati oggetto di trasferimento nei Paesi al di fuori dell'Unione Europea sono anonimizzati inoltre i dati se pur di categoria particolare (indirizzo IP, ecc..) non hanno un impatto rilevante nei confronti della sfera giuridica privata degli interessati.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, in quanto la tutela offerta dagli stessi contratti stipulati permette di limitare qualsiasi violazione ad alto impatto. La diffusione involontaria dei dati causerebbe un danno all'immagine di Microsoft nel contesto globale, la stessa società è impegnata nella sicurezza in modo preponderante.

Valutazione: Accettabile

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Diffusione dei dati personali di minori, concernenti le attrezzature utilizzate dagli stessi per l'utilizzo di servizi offerti dai Responsabili del Trattamento

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Negazione del diritto all'oblio, rischio arginabile in quanto è possibile presentare ricorso all'autorità di garanzia europea e statunitense.

Quali sono le fonti di rischio?

La fonte di rischio risiede nello stesso trasferimento dati, i dati trasferiti sono dati di tipo particolare.
rischio arginabile in quanto l'impatto sulla sfera privata dell'interessato è minimo. Le informazioni riguardano i device utilizzati e pertanto il dato oggetto di rischio è minimo.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Anonimizzazione, VPN, Firewall.

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile, Il rischio è da ritenere trascurabile in quanto i dati oggetto di trasferimento nei Paesi al di fuori dell'Unione Europea sono anonimizzati inoltre i dati se pur di categoria particolare (indirizzo IP, ecc..) non hanno un impatto rilevante nei confronti della sfera giuridica privata degli interessati.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, in quanto la tutela offerta dagli stessi contratti stipulati permette di limitare qualsiasi violazione ad alto impatto. La diffusione involontaria dei dati causerebbe un danno all'immagine di Microsoft nel contesto globale, la stessa società è impegnata nella sicurezza in modo preponderante.

Valutazione: Accettabile

Perdita di dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Diffusione dei dati personali di minori, concernenti le attrezzature utilizzate dagli stessi per l'utilizzo di servizi offerti dai Responsabili del Trattamento

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Negazione del diritto all'oblio, rischio arginabile in quanto è possibile presentare ricorso all'autorità di garanzia europea e statunitense.

Quali sono le fonti di rischio?

La fonte di rischio risiede nello stesso trasferimento dati, i dati trasferiti sono dati di tipo particolare.
rischio arginabile in quanto l'impatto sulla sfera privata dell'interessato è minimo. Le informazioni riguardano i device utilizzati e pertanto il dato oggetto di rischio è minimo.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Anonimizzazione, VPN, Firewall.

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile, Il rischio è da ritenere trascurabile in quanto i dati oggetto di trasferimento nei Paesi al di fuori dell'Unione Europea sono anonimizzati inoltre i dati se pur di categoria particolare (indirizzo IP, ecc..) non hanno un impatto rilevante nei confronti della sfera giuridica privata degli interessati.

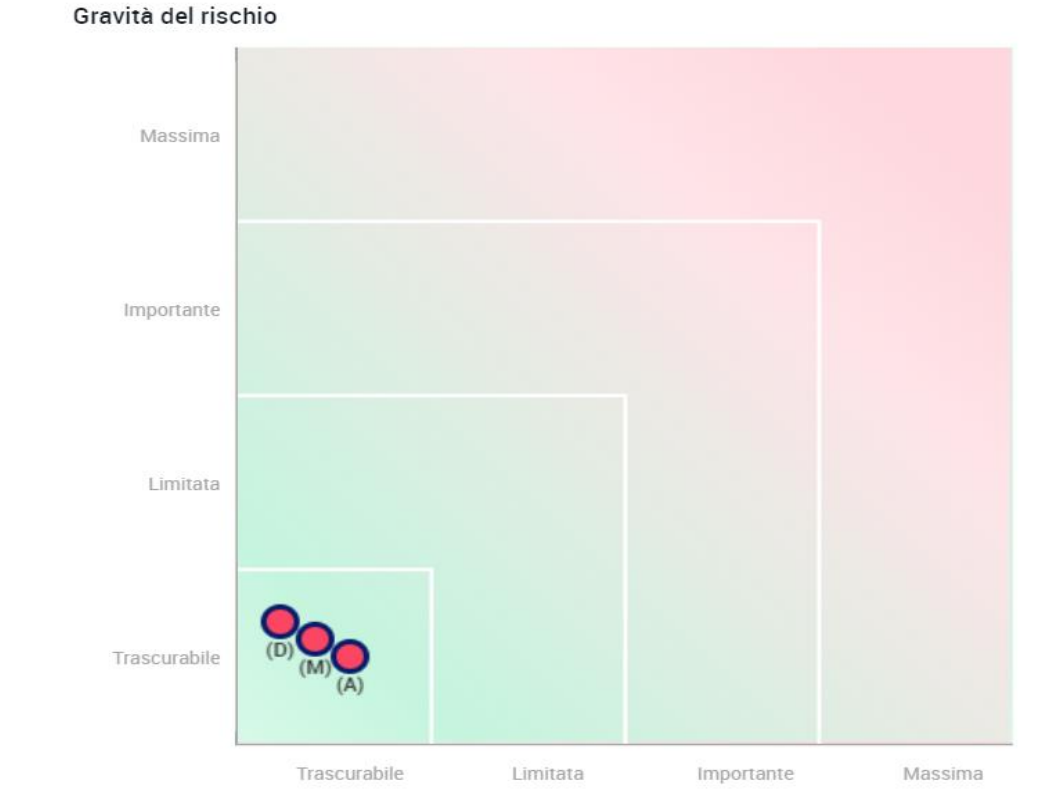
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, in quanto la tutela offerta dagli stessi contratti stipulati permette di limitare qualsiasi violazione ad alto impatto. La diffusione involontaria dei dati causerebbe un danno all'immagine di Microsoft nel contesto globale, la stessa società è impegnata nella sicurezza in modo preponderante.

Valutazione: Accettabile

Panoramica dei rischi

Mappa dei rischi



- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

22/03/23

Piano d'azione

Panoramica

Principi fondamentali

- Finalità
- Basi legali
- Adeguatezza dei dati
- Esattezza dei dati
- Periodo di conservazione
- Informativa
- Raccolta del consenso
- Diritto di accesso e diritto alla portabilità dei dati
- Diritto di rettifica e diritto di cancellazione
- Diritto di limitazione e diritto di opposizione
- Responsabili del trattamento
- Trasferimenti di dati

Misure esistenti o pianificate

- Crittografia
- Anonimizzazione

Rischi

- Accesso illegittimo ai dati
- Modifiche indesiderate dei dati
- Perdita di dati

Misure Migliorabili
Misure Accettabili

Il DPO

Esempio Antonio

ANGELINA SAVIANO
30.04.2026 11:14:15 CEST