



**LICEO CLASSICO STATALE "A. CASARDI"**  
**LICEO DELLE SCIENZE UMANE**  
**LICEO MUSICALE**

Via F.do d'Aragona, 100 – 76121 BARLETTA - Tel. 0883531121  
Cod. Fisc. 81003450723 Cod. Univoco UFS8DQ  
Sito web <https://liceocasardi.edu.it>  
e-mail: [bapc01000r@istruzione.it](mailto:bapc01000r@istruzione.it) – [bapc01000r@pec.istruzione.it](mailto:bapc01000r@pec.istruzione.it)



Circolare n. 521

A tutti i docenti

Al personale ATA

Al/Ai responsabili del trattamento dati

Sede centrale via D'Aragona  
Sede succursale via Botticelli

e p.c. al D.S.G.A., dott.ssa A. Dicuonzo

SEDE

Al sito web

**Oggetto: utilizzo di software sicuro, licenziato o autorizzato dalla scuola.**

- Facendo seguito alla nota n. 706 da parte del Ministero dell'Istruzione e del Merito avente come oggetto "Approfondimenti tecnici di supporto per le istituzioni scolastiche" a cura del Dipartimento per le risorse umane, finanziarie e strumentali - Direzione generale per i sistemi informativi e la statistica, in cui si invita ciascuna scuola al rispetto e alla conformità al GDPR relativamente al trattamento ed al trasferimento extra UE di dati personali degli utenti delle Istituzioni scolastiche attraverso determinati servizi e piattaforme ICT;
- Tenuto conto della comunicazione n° 5 del 26/03/2023 (prot n° 2546 del 27/03/2023) e della comunicazione n° 6 del 02/04/2023 (prot n° 2695 del 03/04/2023) da parte del DPO della nostra scuola, prof. Giuseppe Chiumeo, che si allegano alla presente;

il Dirigente scolastico, titolare del trattamento dei dati della scuola, invita tutto il personale docente e non docente ad un utilizzo consapevole e responsabile, in ambito scolastico, di tutte quelle app e quei software non riconosciuti negli store ufficiali, non autorizzati dalla scuola o provenienti da fonti sconosciute e di accertarsi che i file <sup>1</sup> in transito in essi non siano conservati in server residenti in zone non europee o comunque non tutelate dal GDPR 679/2016 (tali indicazioni sono reperibili nel contratto di licenza d'uso di ogni software installato – il cosiddetto EULA <sup>2</sup>).

Considerata la particolarità della tematica in oggetto, si confida in un'attenta osservazione delle indicazioni da parte di tutto il personale.

Barletta, 04/04/2023

Il Dirigente Scolastico  
Prof.ssa Serafina Maria S. Ardito  
*Firma autografa sostituita a mezzo stampa  
ai sensi dell'art.3, comma 2, del D.Lgs. 39/93*

<sup>1</sup> Ad esempio software gratuiti che convertono file pdf in file editabili quali Ms Word, Ms Excel, Ms PowerPoint, o qualsiasi altro software didattico che raccolga dati di studenti, famiglie, docenti e fornitori.

<sup>2</sup> L'EULA - End-User License Agreement (in italiano: "accordo di licenza con l'utente finale") è il contratto tra il fornitore di un programma software e l'utente finale. Tale contratto assegna la licenza d'uso del programma all'utente nei termini stabiliti dal contratto stesso. Si tratta di un tipo di contratto di termini di servizio.



Prof. Giuseppe Chiumeo  
RPD-DPO – Responsabile Protezione Dati - Data  
Protection Officer  
Docente di informatica

IT Specialist and Consultant

Docente incaricato presso la Facoltà Teologica Pugliese

IT Security Expert - Esperto in Sicurezza Informatica

Esaminatore e supervisore ICDL

Webmaster

---

Alla c.a. del  
Dirigente Scolastico  
Titolare del trattamento dati

e, p.c. Alla c.a. del/dei  
Responsabile/i del trattamento dati

Barletta, 26/03/2023

**Oggetto: nota MIM Protocollo n. 706 - del 20/03/2023 - AOODPPR - Dipartimento per le risorse umane, finanziarie e strumentali. Riscontro alle richieste di supporto in merito 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. Parere del DPO. Comunicazione n° 5.**

Gent.mo Dirigente Scolastico,  
in riferimento alla nota n. 706 da parte del Ministero dell'Istruzione e del Merito avente come oggetto "Approfondimenti tecnici di supporto per le istituzioni scolastiche" a cura del Dipartimento per le risorse umane, finanziarie e strumentali - Direzione generale per i sistemi informativi e la statistica, espongo quanto segue.

La nota fornisce, unitamente al suo allegato, un utile supporto tecnico per discernere la questione della 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.

Per quanto concerne le diverse piattaforme ICT in possesso ed utilizzate da ogni istituzione scolastica, sia per quanto riguarda la didattica che per le attività organizzative di segreteria, è importante 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).

**Software didattici:** nella maggior parte dei casi, le scuole seguite dal sottoscritto DPO, utilizzano strumenti didattici quali Microsoft o Google che, così come più volte ribadito personalmente e stabilito dall'allegato tecnico, dichiarano, nella propria documentazione ufficiale caricata sui rispettivi siti internet, che il trattamento dei dati, ivi incluso l'aspetto dei trasferimenti transfrontalieri degli stessi, risulti essere conforme rispetto alle norme del GDPR. Dunque per tali strumenti non vi sono problemi alcuni circa la legittimità del trattamento dei dati nei trasferimenti transfrontalieri degli stessi. Per quanto concerne invece l'utilizzo di altre piattaforme didattiche, è necessario assicurarsi il rispetto dei termini di un eventuale trasferimento

transfrontaliero deducibile dal contratto/accordo stipulato con l'azienda fornitrice (in caso di dubbi, è possibile contattare direttamente l'azienda fornitrice ai recapiti da esse indicati nei diversi disclaimer che indicano termini, responsabilità e condizioni di un contratto stipulato tra due singole parti).

**Software organizzativi:** anche i software necessari per le attività organizzative della scuola quali quelli per la gestione della segreteria (servizi di protocollo, mail, gestione del personale, gestione famiglie e studenti, registro elettronico, etc.) devono necessariamente rispettare il requisito di trasferimenti dati transfrontalieri conforme alle norme del GDPR. Anche in questo caso, nella maggior parte dei software utilizzati dalle scuole dal sottoscritto curate, tale garanzia è garantita ed è deducibile dai disclaimer dei contratti sottoscritti con le stesse aziende. In caso di dubbi, è possibile contattare direttamente l'azienda fornitrice ai recapiti da esse indicati.

Suggerisco, per poter avere una check-list delle aziende e dei fornitori che forniscono servizi esternalizzati ed in outsourcing, di rifarsi al *registro del trattamento dei dati*<sup>1</sup> compilato e conservato da ciascuna istituzione scolastica.

**Conservazione documentale circa l'analisi del rischio e la valutazione d'impatto:** lo stesso allegato tecnico alla nota n. 706 precisa inoltre, sulla base del principio di accountability (responsabilizzazione) previsto dal Regolamento UE 2016/679 (GDPR), che *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.*

In relazione a tale punto, come già specificato nelle mie precedenti comunicazioni, non vi sono i presupposti per il sorgere dell'obbligo di redazione della DPIA<sup>2</sup> poiché le istituzioni scolastiche non attuano un monitoraggio sistematico né una profilazione né un trattamento su larga scala dei dati, atteso che il trattamento dei dati personali avviene per le sole finalità istituzionali. Difatti il Garante della Privacy, nel Provvedimento del 26 marzo 2020, ha precisato che la DPIA non è necessaria nel caso in esame perché l'istituzione scolastica non effettua trattamenti di dati personali su larga scala. Precisamente il citato provvedimento chiarisce che "La valutazione di impatto, che l'art. 35 del Regolamento richiede per i casi di rischi elevati, non è necessaria se il trattamento effettuato dalle istituzioni scolastiche e universitarie, ancorché relativo a soggetti in condizioni peculiari quali minorenni e lavoratori, non presenta ulteriori caratteristiche suscettibili di aggravarne i rischi per i diritti e le libertà degli interessati. Ad esempio, non è richiesta la valutazione di impatto per il trattamento effettuato da una singola scuola (non, quindi, su larga scala) nell'ambito dell'utilizzo di un servizio on line di videoconferenza o di una piattaforma che non consente

---

<sup>1</sup> L'art. 30 del Regolamento (EU) n. 679/2016 (di seguito "RGPD") prevede, tra gli adempimenti principali del titolare e del responsabile del trattamento, la tenuta del registro delle attività di trattamento. È un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del RGPD) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento. Costituisce uno dei principali elementi di accountability (responsabilizzazione) del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante. <https://www.garanteprivacy.it/registro-delle-attivita-di-trattamento>

<sup>2</sup> DPIA - Data Protection Impact Assessment – cd "Valutazione di impatto", è una procedura prevista dall'articolo 35 del Regolamento UE/2016/679 (RGPD) che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli. Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi. <https://www.garanteprivacy.it/Regolamentoue/DPIA>

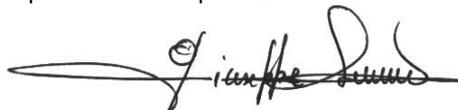
il monitoraggio sistematico degli utenti o comunque non ricorre a nuove soluzioni tecnologiche particolarmente invasive (quali, tra le altre, quelle che comportano nuove forme di utilizzo dei dati di geolocalizzazione o biometrici).”

Ciò non toglie comunque che il titolare del trattamento registri eventuali situazioni di criticità e conservi tutta la documentazione utile a ricostruire le valutazioni condotte al fine di rendicontarne quanto svolto di fronte all’Autorità Garante, ove richiesto. Ricordo che una simile condotta è stata suggerita e fatta adottare dallo scrivente DPO alle diverse istituzioni scolastiche allorquando, nell’aprile 2022, un attacco hacker di tipo *Ransomware*<sup>3</sup> compromise la sicurezza del sistema Axios adottato da un gran numero di scuole: anche in quel caso, pur non avendone l’obbligo, alle scuole fu consigliato di dichiarare e di mettere agli atti la problematica rilevata per eventuali fini ispettivi da parte del Garante della Privacy in un registro di Data Breach.

Alla luce di quanto esposto, in virtù della delicatezza della tematica in oggetto, si raccomanda la massima attenzione ed il massimo rispetto delle indicazioni riportate e, al fine di portare a termine le indagini e le analisi sopra suggerite, consiglio di avvalersi del/i responsabile/i del trattamento dei dati nominati nell’istituzione scolastica nonché dell’animatore digitale, delle funzioni strumentali preposte o dei responsabili dei servizi ICT forniti anche esternamente alle scuole.

Restando a disposizione per ogni eventuale chiarimento in merito, colgo l’occasione per salutarla cordialmente suggerendo anche la frequente consultazione del sito del garante della privacy ([www.garanteprivacy.it](http://www.garanteprivacy.it)).

Prof. Giuseppe Chiumeo  
Responsabile della protezione dei dati della scuola



---

<sup>3</sup> Il ransomware è un programma informatico dannoso ("malevolo") che può "infettare" un dispositivo digitale (PC, tablet, smartphone, smart TV), bloccando l’accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un riscatto (in inglese, "ransom") da pagare per "liberarli".

<https://www.garanteprivacy.it/temi/cybersecurity/ransomware>



Prof. Giuseppe Chiumeo  
RPD-DPO – Responsabile Protezione Dati - Data  
Protection Officer  
Docente di informatica

IT Specialist and Consultant  
Docente incaricato presso la Facoltà Teologica Pugliese  
IT Security Expert - Esperto in Sicurezza Informatica  
Esaminatore e supervisore ICDL  
Webmaster

---

Alla c.a. del  
Dirigente Scolastico  
Titolare del trattamento dati

e, p.c. Alla c.a. del/dei  
Responsabile/i del trattamento dati

Barletta, 03/04/2023

**Oggetto: Utilizzo di software ed APP ufficiali licenziate, rilasciate o autorizzate dalla scuola – comunicazione n° 6.**

Gent.mo Dirigente Scolastico,  
faccio seguito alla mia precedente comunicazione n° 5 del 26/03/2023 relativamente alla nota n. 706 da parte del Ministero dell'Istruzione e del Merito avente come oggetto "Approfondimenti tecnici di supporto per le istituzioni scolastiche" a cura del Dipartimento per le risorse umane, finanziarie e strumentali - Direzione generale per i sistemi informativi e la statistica, per aggiungere quanto segue.

Al fine di rispettare la conformità al GDPR relativamente al trattamento ed al trasferimento transfrontaliero verso Paesi terzi, si invitano tutti i titolari del trattamento dati a non fare utilizzare, per attività scolastiche, APP e software non scaricabili dai diversi store ufficiali (Windows, Android ed IOS) che trattino documenti scolastici con dati personali e particolare (ex sensibili) e di ricordare al proprio personale docente e non docente di assicurarsi, deducendolo dalla relativa licenza software rilasciata (EULA), che i documenti o i dati in essi raccolti non vengano né conservati né fatti transitare su server residenti fuori dall'Unione Europea (si pensi ad esempio ai software gratuiti che convertono file pdf in file editabili quali Ms Word, Ms Excel, Ms PwerPoint, etc o qualsiasi altro software didattico che raccolga dati di studenti, famiglie, docenti e fornitori).

Difatti ricordo che un programma software/app scaricato da fonti non ufficiali potrebbe utilizzare risorse non autorizzate potendo così rubare, manomettere ed inserire in rete dati personali al punto, tali attività, da essere connotabili come cyber-crimini, oltre al controllo del dispositivo e dei file di chi lo abbia installato.

Pertanto La invito a sollecitare docenti e personale ATA ad un utilizzo consapevole di tutte quelle app o software non riconosciuti negli store ufficiali, non autorizzati dalla scuola o provenienti da fonti sconosciute e di accertarsi che i dati/file in esse utilizzati non siano conservati in server residenti in zone non europee o comunque non tutelate dal GDPR 679/2016 (tali indicazioni sono reperibili nel contratto di licenza d'uso di ogni software installato – il cd EULA).

Restando a disposizione per ogni eventuale chiarimento in merito, colgo l'occasione per salutarla cordialmente suggerendo anche la frequente consultazione del sito del garante della privacy ([www.garanteprivacy.it](http://www.garanteprivacy.it)) e, nella speranza di fare cosa gradita, allego una bozza di circolare da far recapitare al Suo personale.

**ALLEGATO**

- Bozza circolare: uso di software consentito.

Prof. Giuseppe Chiumeo  
Responsabile della protezione dei dati della scuola