Progetto Privacy
Privacy Officer Certificati


# RELAZIONE 2023/2024

del Responsabile Protezione Dati Personali

Titolare del trattamento

IC CASTELVETRO

Data: 21/02/2024

## INTRODUZIONE

La scuola, in quanto ente pubblico, rientra nella casistica prevista dalla normativa per la nomina della figura del Responsabile della protezione dei dati (RPD), il quale deve essere nominato obbligatoriamente quando:

a) il trattamento è svolto da un'autorità pubblica o da un organismo pubblico, con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali; oppure
b) le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
c) le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Il Titolare ha quindi provveduto alla nomina di tale figura in Progetto Privacy Srl, referente Giampaolo Spaggiari, Privacy officer certificato TuV e Perfezionato in Data Protection e Data Governance presso l'università "La Statale" di Milano, i cui dati di contatto sono stati pubblicati sul sito internet del titolare.

Il presente documento è l'esito delle attività svolte dal RPD.

## VERIFICHE E CONTROLLI SVOLTI

Le verifiche i controlli si inseriscono nella serie di obblighi in essere per la figura dell'RPD, quale organismo che deve assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento Europeo 2016/679 in materia di protezione dei dati personali di persone fisiche.

Durante l'incarico l'RPD ha informato la scuola circa gli aspetti generali del trattamento dei dati personali e sulle novità in merito e ha fornito supporto e consulenza su alcuni casi critici riportati dall'istituzione scolastica.

Le informazioni e il supporto sono stati forniti sia tramite contatti telefonici che e-mail, con incontri in presenza, online e attraverso webinar gratuiti su specifici argomenti.

Sono state inviate comunicazioni informative sui seguenti argomenti:

- COMUNICATO RPD 2023-01 del 07-03-2023 - Obiettivi di accessibilità
- COMUNICATO RPD 2023-02 del 23-03-2023 - Parere su Nota di supporto MIUR Valutazione di conformità al GDPR del trattamento e trasferimento extra UE di dati personali degli utenti
- COMUNICATO RPD 2023-03 del 19-05-2023 - Nuovo vademecum Garante privacy - Pubblicazioni esiti scrutini e voti
- COMUNICATO RPD 2023-04 del 01-06-2023 - Attestazioni OIV 2023
- COMUNICATO RPD 2023-05 del 13-07-2023 - In vigore nuovo accordo trasferimento dati UE-USA
- COMUNICATO RPD 2023-06 del 04-08-2023 - Istruzioni privacy per inizio anno scolastico 2023-2024
- COMUNICATO RPD 2023-07 del 29-09-2023 - App e siti di terze parti in uso didattica
- COMUNICATO RPD 2023-08 del 18-10-2023 - Informativa app terze parti e limitazioni applicate da Google dopo il 23 ottobre 2023

Sono stati organizzati i seguenti corsi di formazione su argomenti specifici:

- La sezione Amministrazione trasparente nei siti scolastici – cosa e come pubblicare
- La sezione Amministrazione trasparente nei siti scolastici – rispondere ai rilievi dei revisori

Sono state inoltre svolte le seguenti attività:

- Incontro di verifica e controllo privacy presso la sede dell'istituto tenutosi in data 16/02/2024.
- La formazione privacy del personale scolastico è stata effettuata tramite consegna di lettera di incarico con relative istruzioni privacy e con la messa a disposizione di materiale formativo in formato digitale (manuali, slide).

Sono state effettuate le verifiche sui trattamenti di dati personali posti in essere dal titolare verificandone la liceità e la attinenza alla funzione di istituzione scolastica. È stata verificata e valutata la documentazione privacy in possesso dell'istituto, l'organizzazione delle misure di protezione organizzative, logistiche ed informatiche, i trattamenti effettuati tramite internet, la presenza di apposite procedure per gestire eventuali violazioni di dati personali e di procedure volte a garantire agli interessati i loro diritti, la presenza di soggetti terzi debitamente autorizzati tramite accordi contrattuali che li individuano quali responsabili del trattamento ai sensi dell'art. 28 RGPD, la necessità di condurre una valutazione di impatto privacy.

## STRUTTURA E ORGANIZZAZIONE DEL TITOLARE

La struttura organizzativa è composta dal titolare rappresentato dal Dirigente Scolastico, dalla Segreteria, dal corpo Docente e Collaboratori scolastici. Il Responsabile della Segreteria è il D.S.G.A., referente privacy interno per quanto concerne l'area contabile ed amministrativa.

All'interno della Segreteria i soggetti autorizzati al trattamento sono distribuiti nei vari uffici in base alle funzioni strumentali a loro assegnate.

L'elenco aggiornato dei soggetti autorizzati è reperibile presso la stessa Segreteria.

I soggetti esterni che trattano o possono accedere a dati personali sono stati individuati nei seguenti:

- ditte esterne che svolgono il servizio di assistenza informatica ai pc e reti presso il titolare. Questi soggetti vengono nominati amministratore di sistema tramite un accordo contrattuale di nomina a responsabile del trattamento;
- servizi di assistenza software e hosting relativi ad applicativi online utilizzati dalla Scuola per svolgere le ordinarie funzioni istituzionali. Su queste piattaforme vengono gestiti il registro elettronico e le funzioni relative alla "Segreteria digitale". Per queste funzioni i fornitori producono per loro stessi una nomina contrattuale a responsabile del trattamento, controfirmata dal titolare. In mancanza di questa, la Scuola deve proporre e raggiungere un accordo contrattuale di nomina a responsabile del trattamento;
- esperti esterni assunti per specifiche attività didattiche. Di norma questi soggetti (es. psicologo) svolgono attività come liberi professionisti non comunicando i dati alla scuola, operando così da titolari autonomi del trattamento. Vengono comunque individuati come soggetti autorizzati al trattamento nell'ambito del loro incarico;
- enti esterni i cui dipendenti e collaboratori svolgono funzioni di tutor o educatori degli alunni, venendo a contatto diretto con gli stessi. Questi enti vengono individuati quali responsabili del trattamento (art. 28 GDPR) e hanno l'obbligo di formare e informare i propri dipendenti circa i trattamenti da svolgere per la scuola.

Insieme ai referenti privacy del titolare sono stati analizzati i trattamenti di dati personali posti in essere dall'istituzione scolastica, valutando per ognuno di essi il rischio esistente per i diritti e le libertà delle persone fisiche.

L'istituzione scolastica gestisce e mette in atto trattamenti di dati personali di alunni e genitori, personale scolastico, esperti esterni e fornitori, il cui dettaglio è reperibile nel Registro delle attività di trattamento.

## NORMATIVA PRIVACY APPLICABILE

Si è provveduto a verificare che tutti i trattamenti siano conformi alla normativa privacy vigente, al momento della stampa della presente relazione costituita da:

- Regolamento UE 2016/679 (RGPD)
- D. Lgs. 196/2003 Codice privacy modificato dal D. Lgs. 101/2018 Recepimento RGPD
- Provvedimenti del Garante

L'analisi è stata compiuta anche attraverso la condivisione di una check-list di controllo, strumento di lavoro con cui sia l'RPD che l'istituzione scolastica possono analizzare puntualmente e in dettaglio ogni aspetto del trattamento di dati personali della scuola.

## AZIONI DI SUPPORTO E CONSULENZA EROGATE DURANTE L'INCARICO

- Consulenza su istanza di accesso civico generalizzato

## EVIDENZE PRIVACY

Durante le verifiche sono emerse alcune evidenze relativamente a procedure e documentazione dell'istituto che risultano essere ancora non in linea con quanto prescritto dalla normativa vigente in materia di protezione dei dati personali.

In particolare, si prega di porre attenzione ai seguenti punti:

### NON CONFORMITA' – DA RISOLVERE ENTRO 1 MESE DALLA NOTIFICA

Non presenti.

### AZIONI CORRETTIVE – DA ATTUARE ENTRO 3 MESI DALLA NOTIFICA

1) Si ricorda che è obbligatoria la tenuta del Registro delle attività di trattamento, obbligatorio ai sensi dell'art. 30 del GDPR. L'RPD ha inviato un modello, il Registro è da protocollare e inserire in segreteria digitale, non va pubblicato sul sito (REGISTRI_TDT).
2) È prescritta l'adozione di linee guida e di un registro per le violazioni di dati personali. Il documento è da protocollare e inserire in segreteria digitale, non va pubblicato sul sito (POLICY_VDP, REGISTRI_VDP)
3) Il nuovo codice di comportamento dei dipendenti pubblici, varato nel luglio del 2023, consiglia l'adozione di linee guida circa l'utilizzo degli strumenti informatici scolastici o E-Policy. Il documento può essere personalizzato per essere più aderente alle politiche di utilizzo interne della scuola. Un esempio di e-policy è stata resa disponibile dal Ministero nel seguente sito: https://www.generazioniconnesse.it/site/it/moduli-epolicy/. L'RPD ha messo a disposizione un modello di regolamento o e-policy (file POLICY_RI). Il documento va inviato e fatto conoscere a chi utilizza gli strumenti e le reti informatiche scolastiche, può essere pubblicato sul sito alla sezione Privacy.
4) Si consiglia di verificare la presenza delle nomine a responsabile del trattamento ai sensi dell'art. 28 GDPR per i fornitori dei software utilizzata dalla Scuola e il cui utilizzo prevede il trattamento di dati personali, specificatamente il registro elettronico e la segreteria digitale (NOMRES_MADISOFT)

### SUGGERIMENTI PER IL MIGLIORAMENTO – DA ATTUARE ENTRO 6 MESI DALLA NOTIFICA

1) Si ricorda di aggiornare sul sito internet scolastico alla sezione Privacy le informative aggiornate secondo quanto previsto dall'art. 13 del RGPD (files INFDAT_AL, INFDAT_EF, INFDAT_PS, INFDAT_GWS), già in vostro possesso
2) Si ricorda di aggiornare l'atto di designazione con il nominativo della nuova società (in allegato)

## RACCOMANDAZIONI SU SPECIFICI TRATTAMENTI

Le raccomandazioni si riferiscono a trattamenti di dati personali che la scuola può mettere in atto e su cui occorre porre particolare attenzione.

### GESTIONE DEI DATI PERSONALI BES/DSA/L.104 (DATI PARTICOLARI EX ART. 9 RGPD)

È indispensabile che questi dati, appartenenti a categorie particolari (stato di salute), siano protetti ed accessibili ai soli autorizzati. L'accesso a questi dati, in custodia della segreteria, deve avvenire solo quando sono presenti gli addetti della segreteria. Detto ciò, quando gli addetti sono assenti, i fascicoli vanno conservati in armadi chiusi a chiave.
L'utilizzo della chiavetta USB, non essendo dotata di autenticazione informatica se non cifrata, mette ad alto rischio i dati in essa contenuti che possono essere facilmente sottratti o acceduti da parte di soggetti non autorizzati. Si consiglia quindi di togliere i dati dalla chiavetta (formattandola) e di inserirli all'interno di una chiavetta dotata di cifratura oppure utilizzare un altro dispositivo ad accesso sicuro.

In caso di utilizzo di strumentazione informatica, è indispensabile che l'accesso di ogni utente alla piattaforma sia tracciabile e che si disponga di diversi livelli di autorizzazione. Sarà necessario creare dei gruppi di autorizzazione chiusi relativi a ogni singola classe per la condivisione di dati particolari (DSA, BES, PEI) ed evitare così ulteriori diffusioni. In tal modo si evitano l'utilizzo di altri sistemi di comunicazione non tracciabili e non sicuri (e-mail). Si raccomanda che i files siano protetti da pseudonimizzazione o cifratura.

Si consiglia di comunicare ai genitori/tutori di far consegnare le certificazioni sempre e solo direttamente in segreteria, consegnandola in altri punti non viene assicurata la necessaria protezione, prevista dall'Art. 32 del RGPD, ai dati personali appartenenti a categorie particolari (Art. 9 RGPD).

Particolare attenzione occorre prestare alla pubblicazione online o sulla bacheca del registro elettronico (anche solo visibile alla classe) di elenchi di studenti riportanti la dicitura "BES, DSA o ALUNNO H" o di altri elementi che possano fare riferimento all'appartenenza a queste categorie.

La stessa attenzione è da attuarsi anche nei confronti del personale scolastico: non è ammissibile, ad esempio, pubblicare un piano ferie, visibile a tutti, con la dicitura "104" o analoga per segnalare la fruizione dei benefici derivanti dalla legge 5 febbraio 1992, n. 104, oppure indicare nel Piano delle attività del personale ATA specifici problemi relativi allo stato di salute del lavoratore o di suoi famigliari al fine di giustificare orari differenziati.

### DOCUMENTAZIONE PRIVACY DI ISTITUTO

Occorre preparare e mantenere aggiornata e disponibile in caso di controlli la seguente documentazione:

- Informative art. 13 per gli alunni, il personale scolastico e gli esperti esterni
- Nomine e istruzioni ai soggetti autorizzati: personale ATA, docenti, c. scolastici, tutor
- Registro delle attività di trattamento

- Nomine ai Responsabili del trattamento (registro elettronico, segreteria digitale, ecc.)
- Policy Regolamento per l'uso degli strumenti informatici

La documentazione, una volta preparata, va messa in opera nel seguente modo:

- Pubblicare le informative art. 13 sul sito internet e preparare una procedura di segreteria per consegnarle ai nuovi alunni, personale scolastico ed esperti esterni
- Consegnare le Nomine e istruzioni ai soggetti autorizzati
- Consegnare la Policy Regolamento per l'uso degli strumenti informatici a chi ha accesso al sistema
- Inviare per PEC le nomine ai Responsabili del trattamento

Tutto il personale scolastico che opera e che tratta dati personali all'interno della scuola assume il ruolo di "Soggetto autorizzato". La designazione deve essere chiara per l'incaricato, il quale deve ricevere inoltre delle istruzioni dal titolare su come comportarsi in merito al trattamento dei dati personali.

## GRADUATORIE

Per il principio di minimizzazione, nei documenti che si pubblicano la scuola deve inserire i soli dati necessari alla finalità perseguita. Nella fattispecie, le graduatorie sono state oggetto di un provvedimento del Garante (Registro dei provvedimenti n. 274 del 6 giugno 2013) https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2535862 il quale ha stabilito che gli unici dati personali che occorre pubblicare sono nome e cognome, posizione e punteggio ed eventuali altri dati strettamente necessari all'individuazione del candidato.

La stessa prassi è da seguire quando si pubblicano graduatorie a numero chiuso relative a partecipazione a progetti o per l'ottenimento di benefici: anche in tal caso occorre evitare di pubblicare dati eccedenti degli studenti quali "dati relativi alla dispersione, alle insufficienze, all'isee, alla disabilità ecc.". (*Ordinanza ingiunzione nei confronti di Istituto Comprensivo Statale Crucoli Torretta - 9 luglio 2020)*

## PUBBLICAZIONI DATI PERSONALI SU ALBO PRETORIO ONLINE

L'amministrazione che ha intenzione di pubblicare sull'albo pretorio online un atto contenente dati personali è tenuta a verificare, preliminarmente, anche per i dati comuni, l'esistenza di una norma di legge o di regolamento che prescriva l'affissione di quell'atto all'albo pretorio.

In ogni caso prima di diffondere qualsiasi informazione relativa all'interessato, La scuola deve verificare, sulla base di una valutazione responsabile e attenta, quali dati e informazioni pubblicare, tenendo conto dei limiti posti dai princìpi di pertinenza e non eccedenza. Al riguardo va ricordato che l'Autorità Garante, in più occasioni, ha chiarito che anche la presenza di uno specifico regime di pubblicità, non può comportare alcun automatismo rispetto alla diffusione online dei dati e informazioni personali, né una deroga ai principi in materia di protezione dei dati personali (v. provv. del 25 febbraio 2021, n. 68, doc web 9567429).

## CONCLUSIONI

Le eventuali situazioni a cui porre attenzione sono segnalate all'interno della sezione "Evidenze privacy", con diversa classificazione a seconda della gravità e dell'urgenza dell'intervento richiesto.

Qualora ne siano presenti, preghiamo il titolare di attivarsi quanto prima per risolvere le evidenze emerse, dandone comunicazione al RPD.

Modena, 21/02/2024

Giampaolo Spaggiari

GIAMPAOLO SPAGGIARI
Data Protection Officer | Consulente Privacy
Certificazione registro TUV Italia n° CDP_231
Conforme ISO/IEC 17024-2012

Nota: questo rapporto è stato elaborato sulla base di quanto evidenziato durante l'attività ispettiva; è possibile che esso non evidenzi possibili altre attività, non conformi alla legge. Nel corso dell'audit, sono state attuate tutte le possibili precauzioni per fare in modo che questo rapporto sia accurato, ma non è possibile accettare responsabilità di sorta, anche nei confronti di parti terze, per qualsiasi perdita o danno che possa nascere, in conseguenza delle situazioni e delle valutazioni, evidenziate in questo rapporto.