



Management
System
ISO 9001:2015
www.tuv.com
ID 9000039138



Contatti:
Tel. 02-90601324 - Fax 02-700527180
e-mail info@agicomstudio.it
P.E.C. agicom@pec.agicomstudio.it

Studio AG.I.COM. S.r.l. unipersonale
Sede legale: Via XXV Aprile, 12 - 20070 SAN ZENONE AL LAMBRO (MI)
Direzione e amministrazione: Viale Campania, 12 - 26855 LODI VECCHIO (LO)
Campus: Via Villa Mari, snc - 06035 GUALDO CATTANEO (PG)
P.IVA, C.F. e C.C.I.A.A. 05078440962 - Capitale sociale: 50.000,00 Euro i.v.

San Zenone al Lambro (MI), 01 settembre 2026

Spettabile
ISTITUTO DI ISTRUZIONE
c/a DIRIGENTE SCOLASTICO

OGGETTO Circolare informativa **PRIVACY a/s 2026/27:**

Data Breach SPAGGIARI
Validità deliberazioni a distanza organi collegiali
Modifiche normative in tema di I.A. – Il Digital Omnibus
Relazione annuale del Garante – Le principali violazioni sanzionate commesse dalle scuole

Gentile / Egregio Dirigente, di seguito alcune informazioni utili:

Data Breach SPAGGIARI

(per gli Istituti di Istruzione che hanno adottato la piattaforma **BERGANTINI**)

Nello scorso mese di giugno, il Gruppo Spaggiari Parma è stato vittima di un attacco informatico ai danni del modulo "Modulistica smart di Bergantini" (potenzialmente utilizzato in maniera integrata con il registro CLASSEVIVA) che ha sottratto dati relativi a docenti e allievi delle scuole servite (dati anagrafici e di contatto, certificazioni sanitarie e documentazioni varie, anche definibili come "particolari" - ex. sensibili ai sensi dell'art. 9 G.D.P.R.).

L'attacco è avvenuto sfruttando la più attuale delle tecniche malevoli, quella del "ransomware", ossia l'intrusione nella rete informatica della vittima, l'inoculazione di un malware che ha come conseguenza la cifratura (e talvolta, come sembrerebbe in questo caso la sottrazione) dei dati, determinando quindi la loro indisponibilità fino all'eventuale pagamento, da parte della società malcapitata, del riscatto che consentirebbe (ma come si fa a credere sulla parola a veri e propri criminali) il ritorno in chiaro di tutti gli archivi (senza peraltro avere effetti salvifici sui dati fisicamente esfiltrati, se non un generico e quantomai inaffidabile impegno a non utilizzarli).

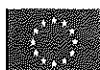
È utile ricordare che, relativamente al pagamento del riscatto, la società Spaggiari ha già dichiarato che non procederà in tal senso.

Nessun dubbio che si tratti di un data breach, almeno per due motivi: in primis la supposta sottrazione dei dati e quindi la fruizione da parte di soggetti non autorizzati e poi l'indisponibilità degli stessi che determina l'impossibilità, per Spaggiari, di garantire appieno i diritti dei soggetti interessati.

Ancor meno dubbi circa il fatto che queste circostanze comportino l'obbligo di annotazione dell'evento sul registro dei data breach, nonché di segnalazione dello stesso al Garante, cose che la società Spaggiari ha dichiarato di aver fatto.

L'obbligo di notifica al Garante nonché di informazione agli interessati spetta al titolare del trattamento dei dati.

Nel caso della piattaforma **BERGANTINI**, tale ruolo è svolto dalla società Gruppo Spaggiari Parma S.p.A. e non dal singolo Istituto di Istruzione, motivo per cui tutti gli adempimenti sono stati eseguiti direttamente dalla società Spaggiari, lasciando libere le scuole da tale incombenza. In qualità di D.P.O. dell'Istituto ho già preso contatti con Spaggiari per avere formale riscontro a tale dichiarazione.



Cofinanziato
dall'Unione europea



Regione
Lombardia

Trattandosi di una questione in divenire, provvederò personalmente a monitorare gli sviluppi e informarla su ogni significativa novità, voglia comunque prendere visione in autonomia della pagina creata da Spaggiari per tenere informate in tempo reale le scuole:

<https://www.spaggiari.eu/news/comunicazione-ufficiale-sull-attacco-informatico-alla-piattaforma-bergantini>

Validità delle deliberazioni a distanza degli organi collegiali

Con nota ministeriale del 30/06 u.s., il M.I.M. ha preso posizione in ordine allo svolgimento a distanza delle attività collegiali a carattere deliberativo, pubblicando un elenco di requisiti tecnico-organizzativi (da verificarsi a cura della scuola) che deve possedere il sistema informatico utilizzato, per la validità formale delle deliberazioni con particolare riferimento a quelle che prevedono una votazione a scrutinio segreto.

È utile precisare che, a dispetto del fatto che si parla di “certificazione” e di “sistemi certificati”, al momento non esiste un albo dei software certificati, né un “certificato di conformità”, ma solamente una serie di requisiti sostanziali, da verificarsi a cura della scuola, che devono essere posseduti dal sistema scelto affinché si possano considerare giuridicamente valide le deliberazioni prese attraverso quel sistema.

Quindi:

- non esiste, almeno nei documenti finora disponibili, una “certificazione MIM”;
- la certificazione ISO 27001, da sola, non certifica la validità del voto;
- la qualificazione ACN del servizio cloud, da sola, non certifica il procedimento deliberativo;
- la presenza su MePA non costituisce certificazione tecnica;
- la semplice dichiarazione commerciale “voto certificato” non è sufficiente;
- la scuola deve acquisire documentazione tecnica e una dichiarazione di conformità del fornitore e poi, ai sensi del punto 9 dell'allegato tecnico, verifica preventivamente l'adeguatezza della soluzione.

Ad oggi abbiamo iniziato ad analizzare alcune piattaforme di voto che sono meglio documentate e che paiono conformi ai requisiti elencati (ELIGO eVoting, SkyVote Meeting / SkyVote Cloud, ClasseViva Ver. Di e Vo.Ce che si appoggiano a ELIGO, VotaFacile e Evoting di Cedat 85) ma non vi è alcun dubbio che anche altre potranno essere giudicate positivamente in futuro.

Importante ricordare che il documento tecnico del M.I.M. permette anche di integrare più strumenti, ad esempio una piattaforma di videoconferenza (Teams, Meet, Forms e relativi sondaggi integrati) e una piattaforma separata di voto, purché il risultato complessivo soddisfi i requisiti, ma in questo caso è necessaria un'analisi più approfondita da eseguirsi di volta in volta al fine di poter dichiarare una sorta di “conformità complessiva”.

Modifiche normative in tema di I.A. – Il DIGITAL OMNIBUS

Il 26 giugno scorso, il Consiglio U.E. ha adottato, con decorrenza 27/07/2026, il c.d. “Digital Omnibus” che razionalizza e semplifica alcune norme in materia di I.A. e di digitalizzazione in generale, contenute nell'A.I. Act.. La modifica più rilevante ha riguardato i sistemi ad alto rischio (in linea di principio non presenti a scuola) per i quali si è posticipata l'entrata in vigore delle regole più stringenti al biennio 2027-2028, mentre non sono stati toccati gli obblighi di trasparenza la cui vigenza è rimasta a far data dal 2 agosto u.s..

Per la maggior parte delle applicazioni scolastiche (chatbot, assistenti alla scrittura, strumenti per la preparazione delle lezioni, sistemi di supporto amministrativo) cambia davvero poco, perché normalmente non rientrano nella categoria ad alto rischio, tuttavia, eventuali sistemi di valutazione automatizzata degli studenti o di profilazione avanzata saranno soggetti a un quadro temporale più lungo.

L'Omnibus inoltre amplia le possibilità di utilizzare ambienti regolamentati di sperimentazione (regulatory sandboxes) e introduce anche meccanismi europei di test controllati, favorendo così le scuole che volessero attuare progetti pilota, sperimentazioni didattiche innovative e collaborazioni con università e centri di ricerca.

Concludendo, per una scuola che ha già adottato o è in procinto di adottare il modello delle Linee guida MIM (governance IA, regolamento IA, formazione, valutazione dei rischi, informativa agli interessati), il Digital Omnibus non impone rivoluzioni organizzative.

Relazione annuale del Garante – Le principali violazioni sanzionate commesse dalle scuole

Prendiamo in prestito dal sito www.tecnicadellascuola.it alcune informazioni contenute in un articolo del 06 luglio scorso nel quale si analizzano le più frequenti condotte poste in essere dagli operatori scolastici che sono stati oggetto di sanzione da parte del Garante:

Diffusione di foto e video di minori online

Un istituto scolastico è stato sanzionato con una multa pecuniaria per aver pubblicato sul proprio canale YouTube un video di auguri di Natale che ritraeva diversi studenti senza aver acquisito un consenso valido, informato ed esplicito. Un altro istituto è stato multato per aver incaricato un influencer di registrare un video promozionale all'interno della scuola. Il video, che ritraeva una studentessa (seppur di spalle), è stato pubblicato sui profili social dell'influencer senza che vi fosse una base giuridica idonea e senza la nomina dell'influencer quale responsabile del trattamento. Un asilo (operante come soggetto sia pubblico che privato) è stato sanzionato con un provvedimento sanzionatorio e prescrittivo per aver pubblicato sul proprio sito web e sul profilo Google Maps numerose immagini di minori in momenti particolarmente delicati (mentre dormivano, a mensa o durante l'igiene personale e il cambio pannolino).

Uso illecito di sistemi di videosorveglianza

Lo stesso asilo sopra menzionato è stato multato anche per aver installato e attivato telecamere di videosorveglianza in aree interne sensibili (come refettorio, bagni, zona riposo e guardaroba) riprendendo i bambini e il personale scolastico senza una previa valutazione di impatto (DPIA) e determinando un monitoraggio a distanza dei dipendenti.

Mailing list e comunicazioni con dati visibili a terzi

Una scuola è stata sanzionata con una sanzione amministrativa pecuniaria per aver inviato una e-mail istituzionale riguardante gli adempimenti vaccinali degli alunni lasciando in chiaro gli indirizzi dei 37 destinatari. In questo modo ha rivelato illecitamente a terzi informazioni sensibili sullo stato di salute e sulle inadempienze vaccinali dei figli di altri genitori. Un altro istituto è stato sanzionato per aver pubblicato sul proprio sito web istituzionale una circolare di convocazione del consiglio di classe straordinario per un procedimento disciplinare contro un alunno: sebbene il nome fosse oscurato nel testo, il cognome del minore era visibile nella denominazione del file allegato consultabile online. Un comune, gestore di un nido e la collegata cooperativa sociale sono stati sanzionati per aver allegato e inviato via e-mail a terzi, in occasione di uno sciopero, un file Excel contenente patologie, disabilità e assegnazione degli insegnanti di sostegno di numerosi alunni.

Mancata protezione dei dati dei lavoratori e dei candidati

Un liceo è stato multato per aver trasmesso i curriculum dei docenti candidati a una selezione interna a quarantaquattro famiglie di studenti a rischio abbandono scolastico affinché potessero scegliere il docente preferito. Un altro istituto è stato sanzionato con una sanzione pecuniaria per aver registrato nel protocollo informatico ordinario (rendendolo visibile a personale non autorizzato di altri uffici) un ricorso relativo alla rettifica del periodo di comportamento di un dipendente, contenente dati sensibili sulla salute e sulla controversia lavorativa. E ancora, un istituto è stato sanzionato per la pubblicazione sul proprio sito web di una graduatoria contenente indirizzi privati e numeri di telefono dei candidati, rimasta poi indicizzata sui motori di ricerca e raggiungibile anche su siti esterni.

Omessa o ritardata nomina del RPD/DPO

Da ultimo un istituto scolastico ha ricevuto una sanzione pecuniaria per aver nominato il nuovo Responsabile della protezione dei dati (RPD/DPO) e averne comunicato i dati al Garante con un notevole ritardo rispetto alla cessazione del precedente incarico.

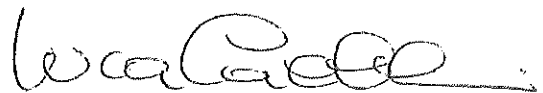
La scuola coinvolta nel caso della circolare con il cognome del minore nel file è stata inoltre sanzionata anche per non aver provveduto a nominare per un certo periodo il RPD e per non averne comunicato i dati di contatto all'Autorità.

Come si vede si tratta di casi molto specifici che segnalano tuttavia la necessità, da parte delle scuole, di porre particolare attenzione anche a piccoli dettagli (come il caso del nome del file) che possono comportare diffusione di dati sensibili.

L'occasione datami dalla presente mi è gradita per porgere i migliori auguri di un sereno e produttivo anno scolastico.

Studio AG.I.COM. S.r.l.

Luca Corbellini – Data Protection Officer



- Acquisiamo il ruolo di D.P.O. della tua scuola;
- Eseguiamo un audit iniziale tramite la piattaforma di Istituto;
- Elaboriamo le informative necessarie;
- Elaboriamo le lettere di autorizzazione;
- Elaboriamo le nomine per i responsabili esterni del trattamento;
- Ci interfacciamo con il tuo Amministratore di Sistema;
- Garantiamo la più ampia consulenza in tutte le questioni inerenti all'applicazione del G.D.P.R. (accesso agli atti, pubblicazioni etc.);
- Formiamo il tuo personale;
- Ti assistiamo nella compilazione della sezione AMMINISTRAZIONE TRASPARENTE;
- Ti forniamo il supporto necessario per implementare l'INTELLIGENZA ARTIFICIALE.

Il D.P.O. giusto per la tua Scuola



Il suo ruolo non è quello di un tecnico che ti configurerà il server, il registro elettronico o la piattaforma didattica digitale, non confonderlo con l'Amministratore di Sistema o di piattaforma, chiedigli piuttosto di collaborare con il tuo personale tecnico e di vigilare sulla corretta applicazione della normativa comunitaria, italiana e dei provvedimenti del Garante.

Accertati della sua competenza tecnico-giuridica, ti potrà tornare molto utile...

Il mondo della scuola è troppo peculiare per farti andare bene chiunque, le sue regole sono specifiche, riguardano in gran parte minori, le materie con cui si dovrà confrontare sono quelle della disabilità, del diritto di famiglia, della somministrazione di farmaci, non rischiare di affidarti a qualcuno che, pur professionale e competente, ha sempre lavorato con le aziende e ha sempre gestito trattamenti di natura commerciale e di marketing.

Accertati della sua esperienza specifica nel mondo della Scuola, farà la differenza...



Studio AG.I.COM. del dott. Corbellini è una società di consulenza in materia di sicurezza sul lavoro e privacy che fin dal 1998 si occupa in modo continuativo e professionale del mondo della scuola.

C'eravamo quando le segreterie si sono informatizzate nei primi anni duemila, affrancandosi dai software ministeriali dopo la concessione dell'autonomia e la nascita degli Istituti Comprensivi e quelli Superiori;

C'eravamo quando la pandemia ha dato il là all'uso massivo delle piattaforme didattiche digitali;

C'eravamo quando MONITORA-PA ha contestato a migliaia di Istituti di eseguire trasferimenti di dati extra-UE in modo illecito;

E ci siamo oggi, al fianco di centinaia di Dirigenti Scolastici in tutta Italia con la passione di oltre 25 anni fa e la competenza maturata in un quarto di secolo di incessante lavoro al servizio della Scuola.

DPO PER LA SCUOLA



SUPPORTO PER
AMMINISTRAZIONE
TRASPARENTE
E INTELLIGENZA
ARTIFICIALE

TROVERAI SUL RETRO TUTTI I DETTAGLI

Acquisizione dell'incarico di D.P.O./R.P.D. della tua Scuola,

Ti assisteremo nella pratica di notifica al Garante dei dati di Luca Corbellini come D.P.O. dell'Istituto.

Incontro tramite la piattaforma di Istituto

Volto ad acquisire tutte le informazioni di base circa la modalità di trattamento dei dati. Lavorando con le scuole da oltre un ventennio sappiamo bene quali dati siano trattati in segreteria, in questo incontro approfondiremo questioni come la collocazione fisica dei dati di personale e allievi, evidenziando quella dei dati più delicati (PEI, PDP, pratiche 104, relazioni con i Servizi Sociali etc.).

In occasione di questo incontro approfondiremo eventuali trattamenti peculiari svolti dal tuo Istituto (gestione di reti di formazione, scuola in ospedale, ristoranti didattici etc.)

Questo incontro sarà preceduto dall'invio di una check-list che vi chiederemo di compilare in cui ci anticiperete una serie di dati anagrafici delle figure apicali, degli amministrativi, delle funzioni strumentali e dei professionisti che collaborano con voi (RSPP, Medico Competente, Psico-pedagogisti etc.).

Trasmissione delle informative di base

In primis trasmetteremo le informative per il personale, gli allievi, i fornitori e il sito internet.

Sarà, in ogni momento, a disposizione il nostro apprezzato servizio di **INFORMATIVA ON DEMAND**, con cui redigeremo tutte le informative che, nel corso dell'anno vi potranno servire, sulla base di alcune semplici domande (CHI vedrà i dati, COSA intendete farci, QUANTO TEMPO resteranno in vista etc.).

Trasmissione delle lettere di autorizzazione e dei contratti di nomina a Responsabile del Trattamento

Sulla base della check-list citata precedentemente, redigeremo per te le lettere di nomina per tutto il personale interno alla scuola (autorizzati) e quelle per gli esterni (responsabili del trattamento).

Interfacciamento con il tuo tecnico

Ci interfacciamo con il tuo Amministratore di Sistema per comprendere il livello di adeguamento dell'infrastruttura informatica di segreteria e gli forniremo le indicazioni previste per le scuole dall'AG.I.D..

Consulenza aperta

In ogni momento, via telefono, mail o videoconferenza, avrete la possibilità di parlare con il D.P.O. o con un suo collaboratore per ogni questione inerente alla riservatezza dei dati personali.

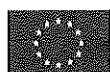
Formazione

Se necessario potremo procedere con la formazione di base del personale di segreteria e dei docenti, così come eseguire la formazione rispetto ai principi di sicurezza informatica da applicare durante l'uso delle piattaforme didattiche digitali e l'alfabetizzazione in materia di intelligenza artificiale (art. 4 A.I. Act).

Forniamo supporto e formazione sulla compilazione della sezione AMMINISTRAZIONE TRASPARENTE

Assistiamo la scuola nell'implementazione consapevole dei sistemi di INTELLIGENZA ARTIFICIALE

[VALUTAZIONE DEI RISCHI SUI SISTEMI IN USO – D.P.I.A. – F.R.I.A. – REGOLAMENTO INTERNO – FORMAZIONE]



Cofinanziato
dall'Unione europea



Regione
Lombardia

Studio AG.I.COM. S.r.l. è un Ente accreditato all'albo di Regione Lombardia per i servizi di istruzione e formazione professionale al n. 1521

Contattaci su commerciale@agicomstudio.it oppure allo 02-90601324