

REGISTRO DELLE ATTIVITA'
DI TRATTAMENTO DATI PERSONALI

ai sensi dell'art. 30 del GDPR 2016/679

Scuola/Organizzazione	**I.I.S. CALOGERO AMATO VETRANO** **Pubblica Amministrazione**

REGISTRO	Paghe

SEDE	Principale C.da Marchesa s.n.c. – 92019 Sciacca (AG)

Data revisione: 21/09/2026

Il presente registro è una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell'art. 30 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Titolare trattamento dati	Cognome	Librici
	Nome	Nellina
	E-mail	Agis01200a@istruzione.it
	PEC	Agis01200a@pec.istruzione.it
	N° telefono	

Responsabile protezione dati (DPO)	Cognome	Furnari
	Nome	Calogero
	E-mail	info@studiofurnari.cm
	PEC	furnariconsulting@pec.it
	N° telefono	092220896

q

TRATTAMENTO: Gestione del personale

Struttura	Sede legale

Personale coinvolto	
Persone autorizzate	Maria Minacori Bono Calogero Sarullo Vincenzo
Clienti / Fornitori	
Altro	

Processo di trattamento	
Descrizione	Politica aziendale che riguarda la gestione del personale in merito a: assunzione, attività formative, valutazioni, pagamenti, ecc
Finalità del trattamento	Reclutamento, selezione, valutazione e monitoraggio del personale: collocazione personale dipendente all'estero Gestione del personale Reclutamento, selezione, valutazione e monitoraggio del personale: formazione professionale
Tipo di dati personali	Lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione professionale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Personali

Categorie di interessati	Clienti ed utenti Potenziali clienti
Categorie di destinatari	Enti pubblici economici Alte amministrazioni pubbliche Consulenti e liberi professionisti anche in forma associata Responsabili esterni Responsabili interni Autorità di vigilanza e controllo Enti previdenziali ed assistenziali
Informativa	Si
Consenso	Non necessario
Profilazione	Non necessario
Dati particolari	Non presenti
Frequenza trattamento	Mensile
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Argo	**Struttura esterna**
Sede di riferimento	**Argo Software srl**
Strutture informatiche di archiviazione Argo Esterna	
Argo	Struttura Esterna
Sede di riferimento	Argo software Srl
Personale con diritti di accesso	
Strutture informatiche di backup	**Argo Esterna**
Argo	Struttura Esterna
Azienda proprietaria	Argo software Srl
Frequenza di backup	1 giorni
Tempo di storicizzazione	7 giorni
Personale con diritti di accesso	
Note	

VALUTAZIONE DEL LIVELLO DI RISCHIO

PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Improbabile	Marginali	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Sono applicate procedure di disaster recovey che garantiscono il ripristino dell'accesso ai dati in tempi ridotti.
- Sono definiti i ruoli e le responsabilità.
- Sono utilizzati software antivirus e anti intrusione.
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Sono gestiti i back up
- Viene eseguita opportuna manutenzione.