

BOZZA — modello tecnico non ancora validato da un legale. Da compilare (dati Votify) e far validare prima dell'uso reale.

Accordo sul trattamento dei dati personali (DPA)

Nomina a Responsabile del trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679

⚠ Modello da validare da un legale prima della firma. Compilare le parti [...].

tra

[ISTITUZIONE SCOLASTICA], codice meccanografico [CODICE], con sede in [INDIRIZZ0], C.F. [C.F.], in persona del Dirigente Scolastico pro tempore [NOME] (di seguito il “**Titolare**”);

e

[VOTIFY — RAGIONE SOCIALE], P.IVA [P.IVA], con sede in [SEDE], PEC [PEC], in persona del legale rappresentante [NOME] (di seguito “**Responsabile**” o “**Votify**”);

di seguito congiuntamente le “**Parti**”.

Premesse

- Il Titolare utilizza la piattaforma **Votify** per lo svolgimento di votazioni degli organi collegiali a distanza (collegi docenti, consigli, scrutini, ecc.).
- Nell'erogazione del servizio, Votify tratta dati personali **per conto del Titolare**, che ne resta l'unico Titolare del trattamento.
- Il presente Accordo disciplina tale trattamento ai sensi dell'art. 28 GDPR e costituisce parte integrante del contratto di servizio tra le Parti.

1. Oggetto, durata, natura e finalità

Votify tratta i dati personali **esclusivamente** per erogare il servizio di voto elettronico: composizione dell'elenco degli aventi diritto, invio degli inviti e dei codici di conferma (OTP), raccolta e conteggio dei voti, generazione del verbale/certificato, e cancellazione dei dati secondo i tempi di cui all'art. 6. La **durata** del trattamento coincide con quella del contratto di servizio.

2. Categorie di interessati e di dati

Interessati: docenti e altri componenti degli organi collegiali aventi diritto di voto; amministratori della scuola che accedono alla piattaforma.

Categorie di dati personali (dati comuni; nessun dato “particolare” ex art. 9 è richiesto dalla piattaforma):

Dato	Trattamento
Nome, cognome	Cifrato a riposo (AES-256-GCM)
Email istituzionale	Cifrata; usata per inviti e OTP
Ruolo (Docente, DS, DSGA...)	In chiaro (non identificativo da solo)
Codice fiscale (facoltativo)	Cifrato; non richiesto per il voto segreto
Preferenza espressa	Solo voto palese (verbale nominale). Nel voto segreto NON è trattata come dato personale : architettura zero-knowledge (art. 4)
Pseudonimo voter_hash (HMAC dell'email)	Per lookup senza esporre l'email

3. Istruzioni documentate del Titolare

Votify tratta i dati **solo** su istruzione documentata del Titolare, costituita dal presente Accordo, dal contratto e dalle funzionalità della piattaforma. Votify **non** utilizza i dati per finalità proprie, non li cede a terzi e non li trasferisce fuori dall'UE (art. 8).

4. Segretezza del voto (architettura zero-knowledge)

Per le votazioni segrete la piattaforma è progettata perché **l'identità del votante e la preferenza espressa non siano mai registrate insieme**: chi ha votato è tracciato per impedire il doppio voto, ma la preferenza confluisce in un conteggio **aggregato** senza alcun riferimento alla persona. Di conseguenza, per il voto segreto **non esiste un dato personale "preferenza"** che possa essere associato all'interessato, nemmeno da Votify.

5. Riservatezza, sicurezza e misure tecniche (art. 32)

Votify garantisce che le persone autorizzate al trattamento siano vincolate alla riservatezza e adotta le misure tecniche e organizzative descritte nella **Scheda tecnica di sicurezza** (documento 04), che costituisce **Allegato B** al presente Accordo. Le misure principali: cifratura delle PII a riposo, TLS in transito, autenticazione senza password (magic link), OTP solo come hash, minimizzazione e cancellazione automatica, isolamento multi-tenant, controllo accessi (RBAC), difese anti-abuso.

6. Conservazione e cancellazione (art. 5.1.e)

Dato	Conservazione
Aventi diritto (PII) — voto segreto	Cancellati alla chiusura della sessione e generazione del certificato (<i>wiping</i>)
Aventi diritto (PII) — voto palese	Confluiscono nel verbale nominale , conservato dal Titolare
Conteggi aggregati (results)	Permanenti, non personali
Certificato/verbale firmato	Scaricabile per una finestra breve (default 90 gg), poi rimosso dai sistemi Votify; la conservazione a lungo

Dato	Conservazione
	termine è del Titolare
Dati volatili (OTP, inviti, sessione)	Auto-cancellazione a TTL breve (minuti/ore)

Al termine del contratto, Votify **cancella o restituisce** tutti i dati personali su scelta del Titolare, salvo obblighi di legge.

7. Sub-responsabili (art. 28.2 e 28.4)

Il Titolare **autorizza** Votify a ricorrere ai sub-responsabili elencati nell'**Allegato A**. Votify impone loro, contrattualmente, obblighi di protezione dei dati equivalenti a quelli del presente Accordo e resta responsabile del loro operato. Votify comunica con congruo preavviso ogni variazione, consentendo al Titolare di opporsi.

8. Trasferimenti extra-UE

I dati sono trattati e conservati **nell'Unione Europea** (Italia). Votify non effettua trasferimenti verso paesi terzi salvo garanzie adeguate ex Capo V GDPR e previa informazione al Titolare.

9. Assistenza al Titolare

Votify assiste il Titolare, con misure adeguate, per: rispondere alle richieste degli interessati (artt. 15-22); garantire sicurezza (art. 32), notifica violazioni (artt. 33-34), DPIA e consultazione preventiva (artt. 35-36). Per il voto segreto molte richieste (es. cancellazione) sono soddisfatte per costruzione.

10. Violazioni dei dati (data breach)

Votify **notifica al Titolare senza ingiustificato ritardo e comunque entro [48] ore** dalla conoscenza di una violazione, fornendo le informazioni utili affinché il Titolare possa adempiere agli artt. 33-34.

11. Audit

Votify mette a disposizione del Titolare le informazioni necessarie a dimostrare la conformità e consente **audit**, anche tramite terzi incaricati, con ragionevole preavviso e nel rispetto della riservatezza. Eventuali certificazioni (es. ISO/IEC 27001, quando ottenute) valgono come evidenza.

12. Durata ed efficacia

Il presente Accordo ha efficacia dalla sottoscrizione e per tutta la durata del trattamento. In caso di conflitto con il contratto di servizio, prevale il presente Accordo per le materie di protezione dei dati.

Luogo e data: _____

Il Titolare (Dirigente Scolastico) _____

Allegato A — Elenco dei sub-responsabili

Aggiornare all’atto della firma con i fornitori effettivi.

Sub-responsabile	Ruolo	Sede / Data residency	Dati trattati
Civo Ltd	Hosting cloud: applicazione, database (MySQL in-cluster, cifrato) e cache Redis	Data center in Germania (UE) ; società con sede nel Regno Unito (vedi nota)	Tutti i dati di servizio (PII cifrate a riposo)
Brevo (Sendinblue SAS)	Invio email transazionali (magic link, inviti al voto, codici OTP)	Francia (UE)	Indirizzo email istituzionale del destinatario e contenuto del messaggio (link di accesso / OTP). Solo API transazionale : nessun contatto marketing; Brevo conserva log transazionali per un periodo limitato
Stripe Payments Europe Ltd	Gestione pagamenti dell’abbonamento	UE (Irlanda)	Nessun dato di voto ; solo dati di fatturazione dell’istituto; nessun dato di carta tocca Votify (PCI-DSS su Stripe)
TopHost (Seeweb S.r.l.)	Hosting della landing page <code>votify.it</code> , gestione DNS e casella email <code>info@votify.it</code> (mittente)	Italia (UE)	Nessun dato personale dei votanti (solo il sito vetrina e i record DNS)

Nota su Civo (jurisdiction): i dati risiedono nell’UE (data center di Francoforte, Germania), ma **Civo Ltd è una società del Regno Unito** (paese terzo post-Brexit, coperto da decisione di adeguatezza UE). Da valutare, in ottica PA/qualificazione ACN, l’eventuale spostamento su un cloud UE qualificato (vedi `COMPLIANCE.md`). Le PII sono comunque **cifrate a riposo** (AES-256-GCM) con chiave detenuta solo nell’applicazione.

Allegato B — Misure tecniche e organizzative

Coincide con la **Scheda tecnica di sicurezza** (documento `04` del kit).