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

Valutazione d’impatto sulla protezione dei dati (DPIA)

Sistema di voto elettronico per organi collegiali — piattaforma Votify

(art. 35 Regolamento UE 2016/679)

> ⚠️ **Bozza precompilata a supporto del Titolare (la scuola).** La DPIA è un documento del **Titolare**, che la adotta con il proprio **DPO**. Votify fornisce qui la parte tecnica e l’analisi dei rischi, già istruita. Completare le parti `[...]` e far validare dal DPO.

---

1. Perché la DPIA è necessaria

Un sistema di **voto elettronico** rientra tra i trattamenti a **rischio elevato** (valutazione sistematica, larga scala nel contesto della comunità scolastica, dati che richiedono particolare tutela per la segretezza del voto). Ai sensi dell’art. 35 GDPR e delle liste del Garante, la DPIA è **dovuta prima dell’avvio**.

2. Titolare, responsabili, DPO

- **Titolare**: `[ISTITUZIONE SCOLASTICA]`.
- **Responsabile del trattamento**: `[VOTIFY]` (accordo art. 28 — doc. `01`).
- **Sub-responsabili**: hosting cloud + database (Civo, data center Germania/UE), provider email (Brevo, Francia/UE), gestore pagamenti (Stripe, Irlanda/UE; nessun dato di voto). Dettaglio e sedi nell’Allegato A del doc. `01`.
- **DPO del Titolare**: `[NOME/CONTATTI]`.

3. Descrizione sistematica del trattamento

Finalità: svolgimento delle votazioni degli organi collegiali a distanza, con formazione del verbale/certificato.

Flusso dei dati: 1. L’amministratore carica l’elenco degli aventi diritto (nome, cognome, email istituzionale, ruolo, CF facoltativo). 2. Alla pubblicazione, ogni avente diritto riceve un invito via email. 3. In cabina, l’identità è confermata con un **OTP** sulla casella istituzionale. 4. **Voto segreto**: emissione di un *ballot token* anonimo; il voto confluisce in un conteggio aggregato. **Voto palese**: registrazione nominale. 5. Alla chiusura: generazione del certificato firmato; **cancellazione** delle PII (voto segreto).

Categorie di dati: vedi doc. `02` §2. **Nessun dato particolare (art. 9)**.

Destinatari: personale autorizzato della scuola, Responsabile e sub-responsabili UE. **Conservazione**: vedi doc. `01` §6. **Data residency**: Italia (UE).

4. Valutazione di necessità e proporzionalità

- **Base giuridica**: compito di interesse pubblico (art. 6.1.e).
- **Minimizzazione**: si raccolgono solo i dati necessari; il CF è facoltativo ed escluso dal voto segreto; la preferenza non è personale nel voto segreto.
- **Limitazione della conservazione**: cancellazione automatica post-seduta.
- **Trasparenza**: informativa ai docenti (doc. `02`).
- **Diritti**: esercitabili verso la scuola; automatici nel voto segreto.

5. Analisi dei rischi per i diritti e le libertà

#	Rischio	Probabilità	Impatto	Misure di mitigazione	Rischio residuo
R1	**De-anonimizzazione del voto segreto**	Bassa	Alto	Architettura zero-knowledge: identità e preferenza mai insieme; `jti` casuale non mappato; conteggi aggregati; `open_text` vietato nel voto segreto	Basso
R2	Accesso non autorizzato ai dati (dump DB)	Bassa	Alto	Cifratura AES-256-GCM delle PII con chiave fuori dal DB; TLS; accesso ristretto	Basso
R3	Correlazione temporale OTP↔voto dai log	Bassa	Medio	Log senza IP dei votanti; timestamp arrotondati; log non incrociabili	Basso
R4	Doppio voto / brogli	Bassa	Alto	Barriera atomica su DB + token monouso anti-riuso; OTP monouso	Molto basso
R5	Furto identità (accesso casella)	Media	Medio	Possesso link + OTP sulla casella istituzionale; limite intrinseco dichiarato	Medio

#	Rischio	Probabilità	Impatto	Misure di mitigazione	Rischio residuo
R6	Perdita/indisponibilità del servizio durante la seduta	Media	Medio	Ridondanza (più repliche), backup, SLA; `[definire RTO/RPO]`	Medio
R7	Violazione da parte di un sub-responsabile	Bassa	Alto	Sub-responsabili UE con obblighi equivalenti; dati cifrati	Basso
R8	“Resurrezione” di PII cancellate dai backup	Bassa	Medio	Retention dei backup coerente col wiping `[definire]`	Basso
R9	Accesso extra-UE / giurisdizione	Bassa	Alto	Dati nell’UE (data center Germania); PII cifrate a riposo; nota: Civo Ltd è società UK (adeguatezza UE) — valutare cloud UE qualificato per la PA (vedi `COMPLIANCE.md`)	Basso

6. Misure di sicurezza adottate

Rimando integrale alla **Scheda tecnica di sicurezza** (doc. `04`).

7. Consultazione del DPO e degli interessati

Parere del DPO: `[da inserire]`. Eventuale consultazione dei rappresentanti degli interessati: `[se applicabile]`.

8. Esito e decisione

Alla luce delle misure adottate, il rischio residuo complessivo è valutato **[basso/accettabile]**. `[Il Titolare decide se avviare / se è necessaria la consultazione preventiva del Garante ex art. 36, di norma non necessaria se il rischio residuo è basso.]`

9. Punti aperti / azioni

- ☐ Definire e documentare la **retention dei backup** (R8).

- ☐ Definire **SLA, RTO/RPO** e piano di continuità (R6).
- ☐ Valutare misure aggiuntive contro la correlazione temporale (R3) per sedute a bassa affluenza.
- ☐ Rivedere la DPIA a ogni modifica sostanziale.

Data: `[DATA]` — Titolare `[ISTITUZIONE]` — DPO `[NOME]` — con il supporto tecnico di `[VOTIFY]`.