Votify

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**: **Equolity S.r.l.s.** (P.IVA 02816500744) — prodotto **Votify** (votify.it) — (accordo art. 28 — doc. `01`).
- **Sub-responsabili**: hosting cloud + database (**AWS eu-south-1, Milano, Italia/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 (l’amministratore sceglie, per ogni votazione, uno dei due canali di accesso): 1. L’amministratore carica l’elenco degli aventi diritto (nome, cognome, email istituzionale, ruolo, CF

facoltativo). 2. Autenticazione del votante: - **Canale Email + OTP**: alla pubblicazione ogni avente diritto riceve un invito via email; in cabina l'identità è confermata con un **OTP** monouso sulla casella istituzionale. - **Canale Google + passkey (SSO)**: nessuna email. Il docente si autentica con l'account **Google** istituzionale (OIDC: Google verifica l'identità e restituisce l'email) e conferma con una **passkey WebAuthn** del proprio dispositivo (2° fattore imposto dall'app). L'eleggibilità si verifica per `voter_hash = HMAC(email)`. Opzionale: **codice di seduta** come presence gate. Votify conserva **solo la chiave pubblica** della passkey (nessun dato biometrico). 3. **Voto segreto**: emissione di un *ballot token* anonimo (identico nei due canali); il voto confluisce in un conteggio aggregato. **Voto palese**: registrazione nominale. 4. Alla chiusura: generazione del certificato firmato; **cancellazione** delle PII (voto segreto). Le chiavi pubbliche passkey persistono per le sedute future e sono soggette a pruning (~15 mesi) / cancellazione all'offboarding.

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)** — AWS eu-south-1, Milano.

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

#	Rischio	Probabilità	Impatto	Misure di mitigazione	Rischio residuo
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	Canale Email: possesso link + OTP sulla casella istituzionale (limite intrinseco dichiarato). Canale **Google + passkey**: **doppio fattore forte** (account Google, con eventuale 2FA della scuola, + passkey legata al dispositivo, phishing-resistant) → rischio **ridotto**	Medio→Basso
R6	Perdita/indisponibilità del servizio durante la seduta	Media	Medio	Ridondanza (più repliche), backup, SLA; RTO ~14 min, RPO ~pochi minuti (testati realmente il 2026-09-13, vedi `allegato_compliance.md`)	Basso
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: 14 giorni, sempre inferiore alla finestra di wiping (90gg) — un backup non può mai far “risorgere” un dato già cancellato dal certificato oltre la retention propria	Basso
R9	Accesso extra-UE / giurisdizione	Bassa	Alto	Dati nell’UE, in **Italia** (AWS eu-south-1, Milano), **qualificata ACN QC2/QI2** (verificato 2026-09-13, vedi	Basso

#	Rischio	Probabilità	Impatto	Misure di mitigazione	Rischio residuo
				`COMPLIANCE.md`); PII cifrate a riposo	
R10	Dipendenza dal provider di identità (Google) nel canale SSO	Bassa	Medio	Google (Ireland Ltd, UE) tratta **solo l'email** per l'autenticazione, **nessun dato di voto**; l'istituto usa il proprio dominio Google Workspace (già suo fornitore); resta sempre disponibile il fallback al canale **Email + OTP**	Basso
R11	Compromissione del registro passkey (chiavi pubbliche)	Bassa	Basso	Sono **chiavi pubbliche**, inutili per impersonare senza il dispositivo fisico e la verifica utente (biometria/PIN); **nessun dato biometrico** è conservato; pruning automatico e reset self-service	Molto 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

- [x] Definire e documentare la **retention dei backup** (R8) — 14 giorni, 2026-09-13.

- [x] Definire **SLA, RTO/RPO** e piano di continuità (R6) — RTO ~14 min, RPO ~pochi minuti, testati realmente il 2026-09-13.
- [ ] 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 **Equolity S.r.l.s.** (Votify).