Votify

Scheda tecnica delle misure di sicurezza

Piattaforma Votify — misure tecniche e organizzative (art. 32 GDPR)

> Documento fornito da **Equolity S.r.l.s.** (P.IVA 02816500744) — prodotto **Votify** (votify.it) — al Titolare. Costituisce **Allegato B** al DPA (doc. `01`). Descrive le misure realmente implementate nella piattaforma. Aggiornare a ogni modifica rilevante e alla data di ogni certificazione.

Versione: `[X.Y]` — Data: `[DATA]`

---

1. Riservatezza dei dati

- **Cifratura delle PII a riposo**: nome, cognome, email e codice fiscale sono cifrati con **AES-256-GCM** a livello applicativo, con **nonce diverso per ogni riga**; la chiave di cifratura (DEK) **non risiede nel database** ma in un gestore di segreti. Un eventuale dump del database è illeggibile senza la chiave.
- **Pseudonimizzazione**: i lookup avvengono tramite `voter_hash` = HMAC-SHA256 dell'email normalizzata, non reversibile senza la chiave.
- **OTP non reversibili**: i codici di conferma sono conservati solo come **hash argon2id**, con TTL di 5 minuti e uso singolo.
- **Cifratura in transito**: **TLS** su tutte le connessioni (client↔servizio, servizio↔database, servizio↔cache); certificati validi (Let's Encrypt).

2. Autenticazione e controllo accessi

- **Accesso amministratore senza password** (magic link monouso, valido 15 min) sulla casella istituzionale registrata: nessuna password da rubare. In alternativa, l'amministratore può accedere via **SSO Google** con la stessa email istituzionale registrata: **stessa radice di fiducia** del magic link (possesso di quell'account), con autenticazione **uguale o più forte** (2FA della scuola, phishing-resistant). L'elevazione ad admin avviene **solo** se l'email è `email_verified` e corrisponde a **una sola** scuola **attiva** (match ambiguo → nessuna elevazione); ogni accesso è tracciato (audit `admin.login.sso`).
- **Sessione** in cookie **HttpOnly, SameSite=Strict, Secure**, con JWT firmato (Ed25519) e scadenza; controllo dell'origine (anti-CSRF).

- **Voto — due canali di autenticazione**, a scelta dell'istituto per ogni votazione:
  - **Email + OTP**: doppio fattore implicito (possesso del link d'invito + OTP monouso sulla casella).
  - **Google + passkey (SSO)**: identità via **OpenID Connect (Google)** con `prompt=select_account` e verifica dell'`id_token` sulle chiavi pubbliche di Google (JWKS: `iss` / `aud` / `exp` / `nonce`); **2° fattore WebAuthn/FIDO2** imposto dall'applicazione (`userVerification=required`), phishing-resistant. La piattaforma conserva **solo la chiave pubblica** della passkey (nessun dato biometrico); il ballot token emesso è **anonimo** e il `cast` viaggia senza cookie identificativo (segretezza invariata). **Codice di seduta** opzionale come presence gate, validato prima dell'emissione della challenge.
- **Anti-abuso**: rate limiting su Redis **per IP e per votante** (il collegio dietro un solo IP non si strozza); reset self-service delle passkey e pruning automatico delle credenziali inutilizzate.
- **Isolamento multi-tenant**: ogni dato è vincolato alla scuola; l'identità del tenant deriva sempre dal token firmato, mai da input del client.

3. Integrità e segretezza del voto

- **Voto segreto (zero-knowledge)**: identità e preferenza non sono **mai** memorizzate insieme; il *ballot token* è anonimo (`jti` casuale non mappato al votante, `aud` legata alla sessione); i conteggi sono **aggregati**.
- **Anti doppio voto**: barriera atomica sul database + token monouso anti-riuso sulla cache.
- **Certificato verificabile**: il verbale è firmato (**JWS Ed25519**) e verificabile pubblicamente e nel tempo tramite chiavi pubbliche (JWKS); qualsiasi alterazione invalida la firma.

4. Minimizzazione e limitazione della conservazione

- Si raccolgono **solo** i dati necessari; il **codice fiscale è facoltativo** ed escluso dal voto segreto.
- **Cancellazione automatica** (wiping) delle PII degli aventi diritto alla chiusura di una votazione segreta; i dati volatili (OTP, inviti, stato sessione) si auto-cancellano a TTL breve.
- Certificato scaricabile per finestra breve (default 90 gg), poi rimosso dai sistemi Votify.

5. Difese contro abusi e attacchi

- **Rate limiting** su più livelli (edge, reverse proxy, applicazione) per IP e per identificatore logico; limiti su dimensione del corpo delle richieste e timeout difensivi.
- **Security headers** (CSP, HSTS, X-Frame-Options DENY, nosniff, Referrer- Policy); **risposta anti-enumeration** sul login.
- **Isolamento di rete** in produzione: politiche di rete *default-deny* con soli flussi minimi consentiti; ruoli con privilegio minimo (RBAC).

6. Gestione dei segreti e delle chiavi

- Chiavi e credenziali **mai** nel codice o nelle immagini: iniettate a runtime come variabile d'ambiente da **AWS Secrets Manager** al lancio del container — mai in chiaro nell'immagine o nel repository.
- **Cifratura at-rest** dello storage dei segreti dell'orchestratore; accesso ai segreti ristretto e auditabile.
- **Rotazione** delle chiavi di firma con mantenimento delle pubbliche storiche (verifica dei verbali passati).

7. Riservatezza dei log

- I log applicativi **non** contengono l'indirizzo IP dei votanti né dati personali; i timestamp degli eventi di voto sono **arrotondati**; i log web sono tenuti separati e non incrociabili con gli eventi di voto.

8. Disponibilità e continuità

- Più repliche dei componenti applicativi, riavvii senza downtime, probe di salute.
- **Backup** del database: giornaliero, retention **14 giorni** (coerente con la finestra di wiping a 90gg del certificato — il backup non estende mai la conservazione oltre quanto già previsto). **RTO/RPO**: RTO misurato con un test di ripristino reale (2026-09-13) = **~14 minuti** (ordine di grandezza, dominato dal tempo di provisioning di una nuova istanza, non dalla dimensione dei dati); RPO ~**pochi minuti** grazie al point-in-time recovery continuo entro la finestra di retention.

9. Data residency e sub-responsabili

- Trattamento e conservazione **nell'UE**: hosting applicazione, **database (Aurora MySQL cifrato) e cache** su **AWS**, regione **eu-south-1, Milano (Italia)** — qualificata **ACN QC2/QI2** (livello critico, vedi `COMPLIANCE.md`). Email transazionali via **Brevo (Sendinblue SAS, Francia)**. Pagamenti su **Stripe** (UE), senza dati di voto e senza dati di carta presso Votify. Landing page e DNS su **TopHost/Seeweb (Italia)**, senza dati dei votanti. Nessun trasferimento di dati **fuori dall'UE**.

10. Organizzazione e processi

- Personale vincolato alla riservatezza e formato.
- Procedura di **gestione delle violazioni** con notifica al Titolare entro `[48]` ore.
- **Vulnerability assessment / penetration test** `[pianificati/eseguiti in data ...]`.
- **Percorso certificazioni**: `[ISO/IEC 27001 — in corso / ottenuta il ...; qualificazione ACN — in corso]`.

Le misure sono soggette a miglioramento continuo. La presente scheda riflette lo stato alla data indicata.