

08

SCHEDA DI SUPPORTO

Scheda di supporto alla valutazione d'impatto, DPIA

Gestione digitale degli organi collegiali e delle operazioni di voto, piattaforme Camelot Voto e Camelot Assemblee. Documento di supporto ai sensi degli artt. 28, par. 3, lett. f) e 35 GDPR e della sezione 6 dell'Allegato tecnico, nota MIM prot. 3803 del 30 giugno 2026.

Società

Camelot S.r.l. SB

Destinatari

Istituzioni scolastiche

Tipo di documento

Documento di supporto

TESTO

Scheda di supporto alla valutazione d'impatto, DPIA

Gestione digitale degli organi collegiali e delle operazioni di voto, piattaforme Camelot Voto e Camelot Assembly. Documento di supporto al titolare ai sensi degli artt. 28, par. 3, lett. f) e 35 GDPR e della sezione 6 dell'Allegato tecnico, nota MIM prot. 3803 del 30 giugno 2026. Versione 2, aggiornata al 6 ottobre 2026.

TRATTAME

Gestione digitale delle sedute degli organi collegiali e delle operazioni di voto mediante le piattaforme Camelot Voto e Camelot Assembly.

TITOLARE

[denominazione dell'istituzione scolastica, codice meccanografico, sede, C.F.]

RESPONSA

Camelot S.r.l. SB, con sede legale in Via Palestro 62, 10015 Ivrea (TO), P. IVA e C.F. 11925790963, Società Benefit.

RIFERIME

Art. 35 del Regolamento UE 2016/679, GDPR; art. 28, par. 3, lett. f), GDPR; sezione 6 dell'Allegato tecnico trasmesso con nota MIM prot. 3803 del 30 giugno 2026; Linee guida WP248 rev. 01 sulla valutazione d'impatto; provvedimento del Garante n. 467 dell'11 ottobre 2018.

VERSIONE

[] Base, accesso e voto tramite collegamento personale e univoco inviato al recapito e-mail di ciascun componente, istituzionale o comunicato all'istituzione. [] Premium, in aggiunta autenticazione forte a due fattori, OTP via SMS e accesso tramite SPID, CIE o CNS.

CAMPI

Le parti tra parentesi quadre sono campi da completare a cura dell'istituzione scolastica, con il supporto del proprio Responsabile della protezione dei dati, DPO.

SEZ. 1 Finalità del documento e istruzioni d'uso

La valutazione d'impatto sulla protezione dei dati, DPIA, è un adempimento del titolare del trattamento. Per il trattamento in esame il titolare è l'istituzione scolastica, che la effettua consultando il proprio DPO ai sensi dell'art. 35, par. 2, GDPR. Camelot S.r.l. SB, in qualità di responsabile del trattamento designato ai sensi dell'art. 28 GDPR, assiste il titolare fornendo con questo documento le informazioni necessarie, in adempimento dell'obbligo di assistenza di cui all'art. 28, par. 3, lett. f), GDPR e della sezione 6 dell'Allegato tecnico.

Il documento è costruito perché l'istituzione possa completare la propria DPIA senza dover ricostruire autonomamente il funzionamento della piattaforma. Le sezioni 3, 4 e 6 descrivono trattamento e misure e sono precompilate dal fornitore; le sezioni 2, 5, 7, 8 e 9 contengono le valutazioni riservate al titolare, con proposte di compilazione da confermare o adattare. Il documento non sostituisce la DPIA né il giudizio del titolare e del suo DPO, costituisce la base informativa e metodologica per redigerla.

SEZ. 2 Verifica preliminare, la DPIA è necessaria?

L'art. 35, par. 1, GDPR richiede la DPIA quando un trattamento, specie se basato su nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Le Linee guida WP248 rev. 01 individuano nove criteri e la presenza di due o più criteri rende di regola necessaria la valutazione. Applicati al trattamento in esame.

TABELLA

CRITERIO WP248	RICORRE	MOTIVAZIONE
Dati relativi a interessati vulnerabili	Sì	Il trattamento riguarda lavoratori, personale docente e ATA, e, nelle elezioni e negli organi con componente studentesca, studenti anche minorenni.
Uso innovativo di tecnologie	Sì	Voto elettronico e gestione telematica di organi collegiali costituiscono applicazione di tecnologie innovative a un procedimento tradizionale.
Dati ad alta componente personale	Sì, in parte	L'espressione di voto attiene alla libertà di opinione. Nel voto segreto la preferenza è anonimizzata in modo irreversibile, ma il dato di partecipazione e il voto palese restano riconducibili.
Trattamento su larga scala	No, limitato	Il perimetro è la comunità scolastica del singolo istituto.
Valutazione o scoring, decisioni automatizzate con effetti giuridici, monitoraggio sistematico, combinazione di insiemi di dati, impedimento all'esercizio di diritti	No	Il conteggio dei voti è l'applicazione deterministica di regole deliberate dall'organo, non una decisione automatizzata ex art. 22 GDPR. Non vi è profilazione né monitoraggio sistematico.

Ricorrono almeno due criteri, interessati vulnerabili e tecnologia innovativa, ai quali si aggiunge il richiamo dell'elenco allegato al provvedimento del Garante n. 467/2018 ai trattamenti effettuati con tecnologie innovative su soggetti vulnerabili, inclusi i minori. La stessa sezione 6 dell'Allegato tecnico prevede che la valutazione d'impatto sia effettuata nei casi previsti, e in particolare per i sistemi di voto digitale.

ESITO

Conclusione proposta, la DPIA è necessaria e va completata prima dell'avvio del trattamento. [Conferma dell'istituzione, sentito il DPO]

SEZ. 3

Ruoli e responsabilità

RUOLO

[Istituzione scolastica], titolare del trattamento, art. 4, n. 7, GDPR.

Determina finalità e mezzi: delibera il regolamento, definisce il registro degli aventi diritto, configura gli eventi, adotta informativa e DPIA, conserva verbali ed evidenze.

RUOLO	[DPO dell'istituzione, nominativo e contatti], responsabile della protezione dei dati del titolare, artt. 37-39 GDPR. È consultato nella redazione della DPIA e ne sorveglia l'attuazione. Il suo parere è riportato nella sezione 8.
RUOLO	Camelot S.r.l. SB, responsabile del trattamento, art. 28 GDPR. Progetta, sviluppa ed eroga la piattaforma. Tratta i dati per conto del titolare sulla base dell'accordo ex art. 28 e delle istruzioni documentate. Canale dedicato, privacy@camelot.vote .
RUOLO	Sub-responsabili, art. 28, par. 4, GDPR. Fornitori di infrastruttura e servizi tecnici autorizzati dal titolare ed elencati nell'Allegato III dell'accordo ex art. 28: infrastruttura cloud AWS in data center UE, monitoraggio tecnico degli errori applicativi tramite Sentry con dati in Germania, recapito SMS e OTP tramite Twilio ove attivata la versione Premium, streaming delle assemblee tramite LiveKit ove attivato, gateway di identità SPID, CIE e CNS e, su richiesta, firma digitale e marca temporale tramite InfoCert S.p.A., recapito PEC tramite Openapi S.p.A. ove attivato.
RUOLO	Presidente, segretario, assistenti, persone autorizzate del titolare, art. 29 GDPR e art. 2-quaterdecies D.Lgs. 196/2003. Operano in piattaforma con ruoli a minimo privilegio. L'istituzione li designa e li istruisce.

SEZ. 4 Descrizione sistematica del trattamento

4.1 Contesto e finalità

Il trattamento consente lo svolgimento a distanza o in forma mista delle attività collegiali dell'istituzione e delle relative operazioni di voto, in due perimetri distinti che l'istituzione disciplina nel proprio regolamento.

- Sedute deliberative degli organi collegiali dei docenti, collegio dei docenti e sue articolazioni, consigli di classe, interclasse e intersezione, ai sensi dell'art. 44, comma 3, lett. a) e b), del CCNL Istruzione e Ricerca 2019-2021 e della nota MIM prot. 3803 del 30 giugno 2026 con relativo Allegato tecnico, nonché di eventuali gruppi di lavoro, nell'ambito dell'autonomia organizzativa dell'istituzione.
- Elezioni telematiche dei rappresentanti, genitori, studenti e altre componenti, disciplinate dal D.Lgs. 297/1994, dall'O.M. 215/1991 e dal regolamento adottato dall'istituzione nell'esercizio della propria autonomia, D.P.R. 275/1999, nel rispetto dei principi di personalità, libertà, eguaglianza e segretezza del voto.

Le finalità sono esclusivamente istituzionali: convocazione e gestione delle sedute, verifica delle presenze e dei quorum, espressione e conteggio del voto, verbalizzazione, produzione e conservazione delle evidenze richieste dalla normativa.

4.2 Flusso del trattamento per fasi

FASE

1. Costituzione del registro degli aventi diritto

L'istituzione carica in piattaforma l'elenco degli aventi diritto per ciascun organo o elezione, secondo i principi di esattezza e minimizzazione, con i soli dati necessari a identificare e contattare.

DATI Nome, cognome, recapito, e-mail e cellulare, categoria e ruolo, eventuale codice identificativo interno.

FASE

2. Convocazione e invito

La piattaforma invia a ciascun avente diritto un collegamento personale e univoco, verificato rispetto al registro. L'uso condiviso o impersonale delle credenziali è impedito.

DATI Recapiti, token personale di accesso.

FASE

3. Identificazione e autenticazione

Accesso con collegamento personale e univoco verificato sul registro degli aventi diritto. Nella versione Premium, secondo fattore OTP usa e getta via SMS e autenticazione forte tramite SPID, CIE o CNS, con integrazione SSO ove configurata. Il livello è scelto dall'istituzione in modo adeguato al rischio della votazione, sez. 3.2 dell'Allegato tecnico. Sessioni a durata limitata, con interruzione automatica alla scadenza, revoca dei token abilitata e accessi registrati. In Camelot Voto e nei componenti per Google Meet e Zoom la stessa persona già autenticata può essere collegata da più dispositivi; il voto, una volta espresso, non è ripetibile da alcun dispositivo o sessione. In Camelot Assemblee una sola connessione attiva per avente diritto: un nuovo accesso chiude la precedente entro circa 30 secondi, con avviso.

DATI Identificativi di accesso, log di autenticazione e di sessione.

FASE

4. Partecipazione alla seduta, Camelot Assemblee

Rilevazione presenze e quorum costitutivo in tempo reale, discussione, interventi in chat, gestione dei punti all'ordine del giorno. Lo streaming audio video può avvenire nella piattaforma oppure sulla piattaforma di videoconferenza già in uso all'istituzione, per esempio Google Meet tramite componente aggiuntivo Camelot. In tal caso i flussi audio video sono trattati nell'ambito del rapporto già in essere tra l'istituzione e il proprio fornitore.

DATI Presenze con orari, ruoli in seduta, contributi in chat, flussi audio video, non registrati salvo diversa decisione dell'istituzione annotata a verbale.

FASE

5. Votazione palese

Espressione del voto riconducibile al votante, come richiesto dalla natura palese della deliberazione. Esiti disponibili per la verbalizzazione.

DATI Identità del votante, espressione di voto, marca temporale.

FASE	6. Votazione a scrutinio segreto La preferenza è cifrata sul dispositivo del votante prima della trasmissione. Autenticazione ed espressione del voto sono separate in modo strutturale e irreversibile. Il sistema registra che l'avente diritto ha votato, ma non conserva in alcun archivio la corrispondenza tra identità e voto. Log e metadati sono gestiti in modo da impedire la re-identificazione anche indiretta. DATI Dato di partecipazione al voto, ha votato o non ha votato. Preferenza anonimizzata e cifrata, non riconducibile.
FASE	7. Scrutinio ed esiti Conteggio automatico senza spoglio manuale. Controllo di univocità, un voto per avente diritto e per quesito, su registro separato dall'archivio delle preferenze. Validazione delle espressioni alla ricezione, gestione separata di bianche, nulle e astensioni, calcolo di validità e maggioranze per singola delibera. Un quesito chiuso non può essere riaperto, l'eventuale ripetizione avviene con nuova votazione. DATI Esiti aggregati. Nel palese, riparto nominativo. Nel segreto, soli totali.
FASE	8. Verbalizzazione e reportistica Il verbale si costruisce durante i lavori, appello, eventi, esiti, note del segretario, ed è finalizzato in forma immutabile con impronta digitale del documento. Verbalì e report possono essere sottoposti a firma digitale e marcatura temporale ed esportati in formati standard, PDF ed Excel, con i relativi metadati. DATI Contenuto del verbale, registro eventi della seduta, esiti.
FASE	9. Conservazione, esportazione, cancellazione Le evidenze restano disponibili all'istituzione per l'esportazione in autonomia durante il servizio. Al termine del rapporto contrattuale i dati sono restituibili in formato standard e sono cancellati decorso il periodo di 30 giorni. Protocollazione, fascicolazione e conservazione a norma dei verbali restano in capo all'istituzione. DATI Tutti i dati del trattamento.
INTERESS.	4.3 Categorie di interessati e di dati Categorie di interessati. Personale docente e dirigente scolastico, personale ATA ove componente degli organi, genitori ed esercenti la responsabilità genitoriale, studenti anche minorenni ove elettori o componenti degli organi, eventuali candidati ed eletti.

DATI

Dati comuni.

Anagrafici essenziali, recapiti, categoria di appartenenza e ruolo, dati di partecipazione, presenze, orari e interventi, dati elettorali, avvenuto voto ed espressione di voto nel solo palese, log tecnici di accesso e sessione, flussi audio video della seduta ove attivati.

DATI

Voto segreto.

La preferenza è anonimizzata in modo effettivo e irreversibile prima della registrazione e non è riconducibile al votante. La piattaforma non conserva la coppia identità e voto in alcun archivio, schermata o report.

DATI

Categorie particolari, art. 9 GDPR.

Non sono richieste né necessarie. In singole deliberazioni palesi l'espressione di voto potrebbe rivelare opinioni dell'interessato, la base è l'art. 9, par. 2, lett. g), GDPR, nel quadro del procedimento deliberativo previsto dall'ordinamento scolastico.

4.4 Destinatari, trasferimenti, conservazione

- **Destinatari.** I dati circolano tra i componenti dell'organo secondo le regole del procedimento, per esempio esiti in seduta e verbale. Non vi è diffusione da parte della piattaforma. Le eventuali pubblicazioni, albo e amministrazione trasparente, restano atti dell'istituzione, nel rispetto del D.Lgs. 33/2013 e del principio di minimizzazione.
- **Sub-responsabili.** Infrastruttura cloud AWS EMEA con data center nell'Unione Europea, regione principale Francoforte, repliche Irlanda, Parigi e Stoccolma. Monitoraggio tecnico degli errori applicativi, Sentry, dati in Germania. Servizi di streaming per le assemblee, LiveKit, USA, Data Privacy Framework e clausole contrattuali tipo. Recapito SMS per l'OTP ove attivato, Twilio, USA, Data Privacy Framework e clausole contrattuali tipo. Gateway di identità SPID, CIE e CNS e, su richiesta, firma digitale e marca temporale dei verbali, InfoCert S.p.A. Recapito PEC ove attivato, Openapi S.p.A. Elenco completo e aggiornato nell'Allegato III dell'accordo ex art. 28 e alla pagina www.camelot.vote/scuole/kit-conformita. Ove la seduta si svolga sulla piattaforma di videoconferenza dell'istituzione, per esempio Google Meet, il relativo trattamento resta nel perimetro del contratto tra istituzione e fornitore di videoconferenza.
- **Trasferimenti extra UE.** Il trattamento avviene in via principale in data center ubicati nell'Unione Europea. Ove singoli servizi accessori comportino trasferimenti verso Paesi terzi, questi avvengono con le garanzie del Capo V del GDPR, decisioni di adeguatezza o clausole contrattuali tipo, come dettagliato nell'Allegato III dell'accordo ex art. 28.

- **Conservazione.** Per la durata del servizio i dati restano nella disponibilità dell'istituzione, che può esportarli in autonomia. Al termine del rapporto contrattuale, restituzione in formato standard e cancellazione decorso il periodo di 30 giorni. I verbali e le evidenze acquisiti agli atti seguono i tempi di conservazione documentale dell'istituzione, [indicare, per esempio permanente per i verbali, secondo piano di conservazione].

SEZ. 5 **Necessità e proporzionalità**

PROFILO **Base giuridica, art. 6 GDPR.**

Art. 6, par. 1, lett. e), GDPR e art. 2-ter D.Lgs. 196/2003, esecuzione di un compito di interesse pubblico dell'istituzione scolastica, quale disciplinato da D.Lgs. 297/1994, D.P.R. 275/1999, art. 44 CCNL Istruzione e Ricerca 2019-2021 e nota MIM prot. 3803/2026 per le sedute, e da D.Lgs. 297/1994, O.M. 215/1991 e regolamento d'istituto per le elezioni telematiche. Per gli eventuali dati ex art. 9, art. 9, par. 2, lett. g), GDPR.

PROFILO **Necessità.**

Ogni dato trattato serve a un requisito dell'Allegato tecnico: identificazione certa, sez. 3, univocità e integrità del voto, sez. 4, sicurezza, sez. 5, verbalizzazione e conservazione, sez. 7. Non sono raccolti dati ulteriori rispetto al procedimento.

PROFILO **Minimizzazione, art. 5.1.c.**

Il registro degli aventi diritto richiede i soli dati identificativi e di contatto. L'istituzione è invitata a non caricare campi ulteriori non necessari. Nel voto segreto la minimizzazione è strutturale, la preferenza è separata dall'identità in modo irreversibile.

PROFILO **Esattezza, art. 5.1.d.**

Il registro è costituito e aggiornato dall'istituzione a ridosso di ciascun evento. Le contestazioni sono gestite dal presidente secondo il regolamento.

PROFILO **Limitazione della conservazione, art. 5.1.e.**

Tempi definiti alla sez. 4.4, nessuna conservazione della corrispondenza tra identità e voto nel segreto, log gestiti per escludere la re-identificazione.

PROFILO **Trasparenza e diritti, artt. 12-22.**

Informativa resa agli interessati con il modello fornito da Camelot, adattato dall'istituzione. Esercizio dei diritti presso il titolare, con assistenza del responsabile. Nel voto segreto i diritti di cui agli artt. 15-20 non si applicano alla preferenza anonimizzata, non essendo l'interessato più identificabile, art. 11 GDPR, e l'informativa lo spiega espressamente.

PROFILO **Assenza di decisioni automatizzate, art. 22.**
Il conteggio automatico applica regole deliberate dall'organo. La volontà collegiale si forma nel procedimento, non in un processo decisionale automatizzato sull'interessato.

PROFILO **Consultazione degli interessati, art. 35.9.**
[L'istituzione valuta se raccogliere il parere delle rappresentanze, RSU, consulta studentesca, comitato genitori, sull'adozione della modalità telematica, dandone atto qui.]

SEZ. 6 **Misure a presidio dei rischi**

Sintesi delle misure tecniche e organizzative attive sulla piattaforma, descritte per esteso nella Documentazione tecnica di rispondenza e nell'Allegato II dell'accordo ex art. 28, cui si rinvia. Le misure sono mappate sulle sezioni dell'Allegato tecnico MIM.

AREA **Identificazione, autenticazione, accessi, sez. 3.**
Identità individuali univoche e non condivise verificate sul registro degli aventi diritto. Collegamento personale univoco. Nella versione Premium, OTP usa e getta via SMS e autenticazione forte SPID, CIE o CNS, con integrazione SSO ove configurata. Controllo accessi basato sui ruoli, Presidente, Segretario, Assistente, Votante, Ospite, a minimo privilegio. Distinzione tra identità e autorizzazione. Sessioni a durata limitata, con interruzione automatica alla scadenza, revoca dei token abilitata e accessi registrati. In Camelot Voto e nei componenti per Google Meet e Zoom la stessa persona già autenticata può essere collegata da più dispositivi; il voto, una volta espresso, non è ripetibile da alcun dispositivo o sessione. In Camelot Assemblee una sola connessione attiva per avente diritto.

AREA **Operazioni di voto, sez. 4.**
Un solo voto per avente diritto e per quesito. Registro degli aventi diritto separato dall'archivio delle preferenze. Validazione delle espressioni alla ricezione. Conteggio automatico senza spoglio. Quesito chiuso non riapribile. Quorum in tempo reale. Gestione separata di bianche, nulle e astensioni.

AREA **Segretezza dello scrutinio, sez. 4.3.**
Cifratura della preferenza sul dispositivo del votante prima della trasmissione. Separazione strutturale e irreversibile tra autenticazione ed espressione. Nessun archivio di corrispondenza tra identità e voto. Log e metadati gestiti contro la re-identificazione anche indiretta. Esito complessivo verificabile senza compromettere la segretezza.

AREA **Sicurezza informatica, sez. 5.**

Comunicazioni cifrate in TLS. Cifratura dei dati e dei backup a riposo. Segregazione degli ambienti in account AWS separati. Registrazione e monitoraggio degli accessi. Vulnerability assessment e penetration test periodici. Tabelle dati replicate in modo asincrono su quattro regioni AWS dell'Unione Europea, Francoforte, Irlanda, Parigi e Stoccolma, e servizi applicativi distribuiti su più regioni; ripristino point-in-time sulla maggior parte delle tabelle di produzione, backup giornalieri cifrati degli archivi di voto conservati 35 giorni e procedure di ripristino nell'ambito del SGSI. SGSI certificato EN ISO/IEC 27001:2022 con estensioni ISO/IEC 27017:2015 e 27018:2019. SaaS qualificato ACN, scheda SA-7041. Amministratori di sistema designati e verificati secondo il provvedimento del Garante del 27 novembre 2008 e seguenti.

AREA **Documenti ed evidenze, sez. 7.**

Verbale finalizzato in forma immutabile con impronta digitale. Firma digitale e marcatura temporale a cura dell'istituzione, con assistenza Camelot e, su richiesta, tramite InfoCert S.p.A. Esportazione in formati standard con metadati. Registro eventi della seduta con data e ora.

AREA **Organizzazione, sez. 8.**

Distinzione applicativa delle funzioni di conduzione e verbalizzazione. Procedura di gestione dei malfunzionamenti con sospensione ed eventuale ripetizione delle operazioni di voto, tracciate nel registro eventi. Modello di regolamento e documentazione a corredo. Assistenza del fornitore secondo il livello attivato.

SEZ. 7 Valutazione dei rischi

Per ciascun rischio sono indicati gli eventi temuti, le misure che lo attenuano e una proposta di valutazione del rischio residuo, probabilità per gravità, che l'istituzione conferma o modifica. Scala: basso, medio, alto, critico.

R1 **Accesso illegittimo o impersonificazione, voto espresso da soggetto diverso dall'avente diritto**

Un soggetto non legittimato potrebbe accedere alla piattaforma o esprimere il voto in luogo dell'avente diritto, per debolezza dei meccanismi di autenticazione, credenziali condivise, link di accesso intercettati, assenza di verifica dell'identità. Incide sulla genuinità della manifestazione di volontà e sulla correttezza della composizione del corpo votante.

MISURE Collegamento personale univoco verificato sul registro. Nella versione Premium, OTP usa e getta via SMS e SPID, CIE o CNS. Blocco delle credenziali condivise. Voto non ripetibile da alcun dispositivo o sessione; nelle assemblee in diretta una sola connessione attiva. Log di autenticazione. Per le votazioni a scrutinio segreto e per le elezioni è raccomandata l'autenticazione a due fattori, versione Premium, in coerenza con la sez. 3.2 dell'Allegato tecnico.

RISCHIO RESIDUO, BASSO [CONFERMARE]

R2

Violazione della segretezza del voto o re-identificazione del votante

L'associazione tra identità del votante e preferenza espressa diviene ricostruibile, in via diretta, log e database non separati, o indiretta, incrocio di timestamp, metadati, esiti in assemblee ristrette. Particolarmente critico quando lo statuto o la legge impongono lo scrutinio segreto. L'impatto sull'interessato è la rivelazione di un'opinione o scelta che aveva titolo a mantenere riservata.

MISURE Cifratura sul dispositivo. Separazione strutturale irreversibile tra identità e preferenza. Assenza di archivi di corrispondenza. Gestione di log e metadati contro la correlazione anche indiretta. Divieto organizzativo di accesso ai dati di voto da parte di amministratori e fornitore.

RISCHIO RESIDUO, BASSO [CONFERMARE]

R3

Alterazione del voto, del conteggio o dell'esito

La modifica, cancellazione o duplicazione dei voti espressi, oppure la manipolazione dell'algoritmo di conteggio o dei risultati pubblicati, per attacco esterno, malfunzionamento o intervento interno non tracciato. Compromette l'esattezza dei dati, art. 5.1.d, e la validità giuridica della deliberazione.

MISURE Validazione alla ricezione. Controllo di univocità su registro separato. Conteggio automatico senza trascrizioni. Quesito chiuso non riapribile. Verbale imm modificabile. Registro eventi.

RISCHIO RESIDUO, BASSO [CONFERMARE]

R4

Indisponibilità del servizio durante seduta o votazione

Interruzione o degrado della piattaforma, guasto, attacco DoS, errore di configurazione, saturazione, in concomitanza con la finestra di voto, con impossibilità per gli aventi diritto di esprimersi. L'impatto è l'esclusione di fatto dall'esercizio del diritto di voto e la potenziale invalidità o ripetizione della seduta.

MISURE Tabelle dati replicate in modo asincrono su quattro regioni AWS dell'Unione Europea e servizi applicativi distribuiti su più regioni; ripristino point-in-time sulla maggior parte delle tabelle di produzione e backup giornalieri degli archivi di voto conservati 35 giorni. Procedura malfunzionamenti con sospensione e ripetizione tracciate. Regolamento dell'istituzione con regole su quorum e ripresa.

RISCHIO RESIDUO, BASSO [CONFERMARE]

- R5 **Perdita o alterazione di verbali ed evidenze**
Distruzione, corruzione o modifica non autorizzata di verbali, log di seduta e risultanze, con perdita della capacità di dimostrare la regolarità del procedimento e l'esito. Rileva anche ai fini dell'accountability, art. 5.2, e della conservazione per il tempo necessario alla tutela in giudizio.
MISURE Cifratura e replica dei backup. Finalizzazione immodificabile. Esportazione in formati standard con metadati. Conservazione documentale a cura dell'istituzione secondo le Linee guida AgID.
RISCHIO RESIDUO, BASSO [CONFERMARE]
- R6 **Abuso di privilegi, lato istituzione o fornitore**
Utenze amministrative dell'ente o del fornitore utilizzate oltre i limiti delle rispettive funzioni, consultazione dei voti, modifica di configurazioni o risultati, accesso ai dati dei votanti, in assenza di segregazione dei ruoli, tracciamento degli accessi privilegiati e istruzioni documentate ex art. 29.
MISURE Ruoli a minimo privilegio. Tracciatura delle operazioni rilevanti. Designazione e verifica annuale degli amministratori di sistema, provvedimento del Garante del 27 novembre 2008. Istruzioni documentate ex art. 28. Audit del titolare.
RISCHIO RESIDUO, BASSO [CONFERMARE]
- R7 **Violazione di dati presso il responsabile o i sub-responsabili**
Rischio di data breach nella catena di trattamento, artt. 28 e 33, riguardante la potenziale compromissione dei sistemi del fornitore della piattaforma o dei suoi sub-fornitori, hosting, comunicazioni, autenticazione, con accesso, perdita o divulgazione non autorizzata dei dati dei votanti. La titolarità del rischio residuo resta in capo al titolare, che dipende dalle misure e dagli obblighi di notifica contrattualmente imposti alla filiera.
MISURE SGSI ISO/IEC 27001:2022. Obblighi contrattuali a catena sui sub-responsabili. Procedura data breach secondo la Data Breach Policy di Camelot, con prima notifica preliminare al titolare entro 1 ora dalla classificazione dell'evento, condizioni di servizio, e notifica con le informazioni ex art. 33, par. 3, GDPR senza ingiustificato ritardo e comunque entro 48 ore, accordo art. 28. Adozione del registro delle violazioni.
RISCHIO RESIDUO, BASSO [CONFERMARE]
- R8 **Eccesso di raccolta o uso ulteriore dei dati**
Raccolta di dati non necessari al voto, dati di navigazione e analytics, o riutilizzo dei dati per finalità diverse e non compatibili, profilazione, statistiche non anonimizzate, finalità commerciali del fornitore, anche mediante conservazione oltre i termini.
MISURE Minimizzazione by design del registro. Finalità limitate contrattualmente. Divieto per il responsabile di trattare per finalità proprie. Cancellazione al termine del servizio.
RISCHIO RESIDUO, BASSO [CONFERMARE]

- R9 **Sicurezza dei dispositivi degli utenti, endpoint security**
Se il dispositivo personale, PC o smartphone, utilizzato dal docente, dal genitore o dallo studente è compromesso, per esempio infetto da keylogger, spyware o malware, l'intento di voto o i contenuti sensibili della riunione potrebbero essere catturati prima che la piattaforma li cifri.
MISURE Sensibilizzazione degli utenti sull'uso di dispositivi aggiornati e protetti da antivirus. Raccomandazione di non utilizzare dispositivi condivisi o pubblici per le votazioni segrete.
RISCHIO RESIDUO, MEDIO, A PRESIDIO DELL'ISTITUZIONE [CONFERMARE]
- R10 **Coercizione, acquisto del voto e privacy dell'ambiente domestico**
Nelle votazioni da remoto viene meno l'isolamento fisico della cabina elettorale. C'è il rischio che un elettore, in particolare uno studente minorenne o un genitore, subisca pressioni, influenze o coercizioni da parte di conviventi durante l'espressione del voto.
MISURE Istruzioni nel regolamento d'istituto e nell'informativa privacy sull'importanza di garantire un ambiente riservato durante il voto.
RISCHIO RESIDUO, MEDIO, A PRESIDIO DELL'ISTITUZIONE [CONFERMARE]
- R11 **Phishing e ingegneria sociale**
Soprattutto nella versione Base, dove l'accesso avviene tramite link univoco via e-mail, malintenzionati potrebbero inviare finte convocazioni contenenti link malevoli per rubare credenziali o installare malware, sfruttando l'urgenza o l'abitudine degli utenti a cliccare sui link istituzionali.
MISURE Campagne di awareness per personale e famiglie su come riconoscere le comunicazioni ufficiali. Forte raccomandazione di adottare la versione Premium, con SPID, CIE o CNS oppure OTP, per le elezioni e le votazioni più critiche.
RISCHIO RESIDUO, BASSO [CONFERMARE]
- R12 **Divario digitale e accessibilità**
Rischio di esclusione dal procedimento democratico e dalla vita scolastica per quelle famiglie o membri del personale privi di adeguata connettività, dispositivi idonei o competenze digitali. A questo si aggiunge il rischio di barriere per utenti con disabilità, per esempio screen reader non supportati, che potrebbe configurare una discriminazione indiretta.
MISURE Previsione nel regolamento di modalità di supporto o alternative per chi è impossibilitato tecnologicamente. Verifica, da parte della scuola, che la piattaforma rispetti i requisiti di accessibilità, per esempio le linee guida WCAG.
RISCHIO RESIDUO, MEDIO, A PRESIDIO DELL'ISTITUZIONE [CONFERMARE]

R13

Rischi legati alle integrazioni di terze parti

In caso di utilizzo di componenti aggiuntivi su piattaforme di videoconferenza già in uso alla scuola, per esempio Google Workspace, potrebbe verificarsi il rischio di intrusioni di esterni nella riunione o di esposizione alle politiche di trattamento dati del fornitore della videoconferenza.

MISURE Configurazione rigorosa delle sale di attesa e dei permessi di accesso da parte del presidente e del segretario. Verifica che l'accordo sul trattamento dei dati tra scuola e fornitore di videoconferenza copra adeguatamente l'uso per gli organi collegiali.

RISCHIO RESIDUO, BASSO [CONFERMARE]

R14

Inesattezza o incompletezza del registro degli aventi diritto

Un registro non aggiornato o errato, aventi diritto mancanti, soggetti non legittimati inclusi, recapiti errati, altera la composizione del corpo votante e incide sulla validità di quorum e deliberazioni, prima ancora dell'intervento della piattaforma. Il registro è costituito e aggiornato dall'istituzione, art. 5.1.d GDPR.

MISURE Costituzione e verifica del registro a ridosso di ciascun evento a cura dell'istituzione. Verifica del collegamento personale rispetto al registro. Gestione delle contestazioni da parte del presidente secondo il regolamento. Correzione degli elenchi prima dell'apertura delle votazioni.

RISCHIO RESIDUO, MEDIO, A PRESIDIO DELL'ISTITUZIONE [CONFERMARE]

I parametri di riferimento per la valutazione della stima della perdita di riservatezza, integrità e disponibilità possono essere desunti dalla tabella che segue.

TERMINI

Per ciascun livello l'impatto sugli interessati è riferito agli stessi termini: perdita di autonomia, esclusione, perdita di libertà, danni fisici, stigmatizzazione, squilibrio di potere, perdita di fiducia, perdita economica.

LIVELLO

1, Basso

RISERVAT.

I dati non presentano particolari requisiti di riservatezza, sono dati pubblici.

INTEGRITÀ

I dati non presentano particolari requisiti di integrità e non fanno parte di transazioni economiche, finanziarie o sanitarie.

DISPONIB.

L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente non comporta multe o penali rilevanti.

INTERESS.

Impatto lieve, per esempio fastidio, sulla vita sociale o personale degli interessati.

LIVELLO	2, Medio	
	RISERVAT.	I dati devono essere riservati per ragioni di business, concorrenza sleale e danni all'immagine, ma un'eventuale diffusione non ha elevati impatti sul business, sul rispetto della normativa vigente o sull'immagine dell'organizzazione.
	INTEGRITÀ	I dati non sono oggetto di transazioni economiche, finanziarie o sanitarie con impatti sul business. La mancanza di integrità non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente.
	DISPONIB.	L'indisponibilità oltre i tempi stabiliti contrattualmente comporta multe o penali non particolarmente rilevanti.
	INTERESS.	Impatto non critico, per esempio perdita di tempo o perdita limitata di serenità.
LIVELLO	3, Alto	
	RISERVAT.	I dati devono essere riservati per ragioni di business e un'eventuale diffusione ha elevati impatti sul business, sul rispetto della normativa vigente o sull'immagine dell'organizzazione.
	INTEGRITÀ	La mancanza di integrità dei dati ha elevati impatti sulle attività operative o sul rispetto della normativa vigente.
	DISPONIB.	L'indisponibilità oltre i tempi stabiliti contrattualmente comporta multe o penali rilevanti.
	INTERESS.	Elevato impatto sulla vita sociale, fino a sconvolgerla, o personale degli interessati.
LIVELLO	4, Critico	
	RISERVAT.	La diffusione delle informazioni ha impatti sul business, sul rispetto della normativa vigente o sull'immagine tali da compromettere la sostenibilità dell'organizzazione.
	INTEGRITÀ	La mancanza di integrità delle informazioni ha impatti tali da compromettere la sostenibilità dell'organizzazione.
	DISPONIB.	L'indisponibilità oltre i tempi stabiliti comporta multe o penali che mettono in pericolo la sostenibilità economica e di immagine o hanno impatti sulla sicurezza delle persone fisiche.
	INTERESS.	Impatto sulla sopravvivenza degli interessati.
Rischi residui che l'istituzione governa direttamente. Qualità e aggiornamento del registro degli aventi diritto, custodia dei dispositivi e dei recapiti personali da parte degli interessati, scelta corretta tra voto palese e segreto secondo regolamento, conservazione a norma dei verbali. Tali profili vanno presidiati con il regolamento, le istruzioni agli autorizzati e l'informativa.		

SEZ. 8 Parere del DPO e consultazioni

CAMPI

Parere del DPO, art. 35, par. 2, GDPR.

[testo del parere oppure rinvio ad atto separato, data e firma]

CAMPI

Eventuale consultazione degli interessati o delle loro rappresentanze, art. 35, par. 9.

[esiti oppure motivi dell'omissione]

SEZ. 9 Esito della valutazione

- ☐ Il rischio residuo per i diritti e le libertà degli interessati è valutato non elevato: il trattamento può essere avviato, con le misure descritte e il piano di riesame di cui alla sezione 10.
- ☐ Il rischio residuo permane elevato: prima dell'avvio è necessaria la consultazione preventiva del Garante ai sensi dell'art. 36 GDPR.

CAMPI

Luogo e data.

[...]

CAMPI

Il Dirigente scolastico, titolare del trattamento.

[nome e firma]

CAMPI

Visto, il DPO.

[nome e firma]

SEZ. 10 Riesame e aggiornamento

La DPIA è riesaminata a ogni modifica sostanziale della piattaforma o del servizio comunicata dal fornitore, a seguito di violazioni di dati o incidenti rilevanti, all'attivazione di nuove funzionalità, per esempio canali di autenticazione, streaming, protocolli end to end, e comunque con cadenza [annuale]. Camelot comunica tempestivamente le variazioni rilevanti ai sensi dell'accordo ex art. 28 e aggiorna la documentazione tecnica a corredo.

SEZ. 11 Documentazione di riferimento

- Allegato tecnico Requisiti tecnico organizzativi per la gestione digitale degli organi collegiali e delle operazioni di voto nelle istituzioni scolastiche, trasmesso con nota MIM prot. 3803 del 30 giugno 2026.
- Documentazione tecnica di rispondenza all'Allegato tecnico e Dichiarazione di conformità della piattaforma Camelot, documenti del fornitore acquisiti agli atti ai sensi della sezione 9 dell'Allegato tecnico.
- Accordo sul trattamento dei dati personali ex art. 28 GDPR con Allegati I-IV, sottoscritto tra istituzione e Camelot S.r.l. SB.
- Modello di informativa agli interessati, artt. 13-14 GDPR, e scheda per il registro delle attività di trattamento, art. 30 GDPR, forniti a corredo.
- Regolamento dell'istituzione per le sedute a distanza e per le elezioni telematiche, procedura di gestione dei malfunzionamenti.
- Linee guida WP248 rev. 01 del Gruppo Art. 29, provvedimento del Garante n. 467 dell'11 ottobre 2018, Raccomandazione Rec(2017)5 del Consiglio d'Europa sui sistemi di voto elettronico.

CHI SIAMO

Camelot è una Società Benefit specializzata in voti digitali e ibridi legalmente riconosciuti e nella conduzione a distanza delle sedute degli organi collegiali.

Società Benefit

Il nostro scopo è assicurare che i sistemi di partecipazione generino un beneficio per le persone e per le comunità. Aiutiamo le organizzazioni a raggiungere gli obiettivi di sostenibilità previsti dall'Agenda 2030.

RICONOSCIMENTI

2019

Nazioni Unite

Invito a parlare della carta dei diritti di cittadinanza digitale.

2020

Pubblicazione scientifica

A Digital Voting System for the 21st Century, D. Casaleggio et al., Springer.

2019

Parlamento europeo

Invito a parlare di cittadinanza digitale e democrazia partecipativa.

2021

Digital Democracy Impact Award

Premio internazionale ricevuto per la piattaforma Rousseau.

🏆 Premio Nazionale Comunicazione Costruttiva

☆ Finalisti Premio Campioni dell'InnovAzione

🏆 Premio Top Digital Company

🌐 Premio ENEA, Enterprise Europe Network

🌐 SPREAD2INNO project

🏆 Premio Camillo e Adriano Olivetti all'Impresa Innovativa e Responsabile

🏆 Premio Città di Pescara

🏆 Premio America Innovazione

🌐 Premio ASviS per l'Anno europeo delle competenze

CERTIFICAZIONI

EN ISO/IEC 27001:2022

ISO/IEC 27017:2015

ISO/IEC 27018:2019

EN ISO 9001:2015

CONTATTI

info@camelot.vote

camelot.vote