

06

KIT ORGANI COLLEGIALI

Accordo sul trattamento dei dati personali (art. 28 GDPR)

Designazione di Camelot S.r.l. SB quale responsabile del trattamento
per l'erogazione delle piattaforme Camelot Voto e Camelot
Assemblee alle istituzioni scolastiche, con Allegati I, II, III e IV.

SEZIONE 6 DELL'ALLEGATO TECNICO, NOTA MIM PROT. 3803 DEL 30 GIUGNO 2026

Società

Camelot S.r.l. SB

Parti

Istituzione scolastica, titolare del trattamento, e Camelot S.r.l. SB, responsabile del trattamento

Natura dell'atto

Atto autonomo di designazione oppure Appendice 1 del contratto di servizio

Contatto privacy

privacy@camelot.vote

Data

6 ottobre 2026 · Versione 2

06

VERSIONE 2 · RILASCIATO IL 6 OTTOBRE 2026

Accordo sul trattamento dei dati personali ai sensi dell'art. 28 GDPR

relativo all'erogazione delle piattaforme Camelot Voto e Camelot Assemblee alle istituzioni scolastiche, per la gestione digitale delle sedute degli organi collegiali e delle operazioni di voto.

NOTA

Il presente accordo può essere sottoscritto come atto autonomo di designazione oppure quale Appendice 1 del contratto di servizio, di cui in tal caso costituisce parte integrante.

PARTI

TRA

L'istituzione scolastica utente del Servizio, come identificata nell'intestazione del contratto di servizio, in persona del Dirigente scolastico pro tempore (di seguito, l'«Istituzione» o il «Titolare»)

E

Camelot S.r.l. SB, con sede legale in Via Palestro 62, 10015 Ivrea (TO), P. IVA e C.F. 11925790963, Società Benefit, in persona del legale rappresentante pro tempore, e-mail privacy@camelot.vote (di seguito, «Camelot» o il «Responsabile»; congiuntamente, le «Parti»)

Premesse

1. L'Istituzione utilizza le piattaforme Camelot Voto e Camelot Assemblee (il «Servizio») per la gestione digitale delle sedute dei propri organi collegiali e delle operazioni di voto, in forza del contratto di servizio in essere (il «Contratto»);
2. L'Allegato tecnico trasmesso con nota MIM prot. 3803 del 30 giugno 2026 richiede, alla sezione 6, che i rapporti tra istituzione scolastica e fornitore siano regolati ai sensi dell'art. 28 del Regolamento UE 2016/679 («GDPR») e, alla sezione 9, che l'istituzione acquisisca la documentazione tecnica e la dichiarazione di conformità del fornitore;
3. nell'erogazione del Servizio Camelot tratta dati personali per conto dell'Istituzione, che determina finalità e mezzi del trattamento in qualità di titolare;
4. anche ove il Servizio sia acquistato per il tramite di un rivenditore o partner commerciale, il presente accordo intercorre direttamente ed esclusivamente tra l'Istituzione e Camelot, e il rivenditore resta estraneo ai dati trattati nella piattaforma;
5. L'Istituzione ha valutato le garanzie presentate da Camelot, ritenendole sufficienti per mettere in atto misure tecniche e organizzative adeguate, come documentato dalle certificazioni e dalla documentazione richiamate nell'Allegato II;
6. L'Istituzione, in qualità di Titolare, garantisce di aver individuato una base giuridica idonea, di aver reso l'informativa agli interessati, di aver adottato la DPIA ove necessaria e di caricare in piattaforma esclusivamente dati esatti, pertinenti e limitati a quanto necessario. Camelot, in qualità di Responsabile, fornisce servizi tecnologici e tratta i dati esclusivamente su istruzione documentata del Titolare, senza alcuna autonomia decisionale sulle finalità o sulla liceità del trattamento.

Tutto ciò premesso, quale parte integrante del presente atto, le Parti convengono quanto segue.

1 Art. 1, definizioni e gerarchia

I termini «trattamento», «dati personali», «interessato», «violazione dei dati personali» e gli altri termini definiti hanno il significato di cui all'art. 4 GDPR. In caso di contrasto tra il presente accordo e il Contratto, prevale il presente accordo per quanto attiene alla protezione dei dati personali.

2 Art. 2, oggetto, natura, finalità e durata del trattamento

Con il presente atto l'Istituzione designa Camelot responsabile del trattamento ai sensi dell'art. 28 GDPR. Il trattamento ha ad oggetto le operazioni, eseguite con strumenti automatizzati, necessarie all'erogazione del Servizio, cioè raccolta, registrazione, organizzazione, strutturazione, conservazione, consultazione, uso, comunicazione ai soggetti legittimati, limitazione e cancellazione.

Le finalità sono esclusivamente quelle stabilite dal Titolare, cioè gestione delle convocazioni, delle presenze e dei quorum, espressione e conteggio dei voti, verbalizzazione, produzione ed esportazione delle evidenze. La descrizione di dettaglio è nell'Allegato I. Il trattamento dura quanto il Contratto, ferme le operazioni di restituzione e cancellazione di cui all'art. 11.

3 Art. 3, istruzioni documentate

Camelot tratta i dati personali soltanto su istruzione documentata del Titolare, anche con riguardo ai trasferimenti verso Paesi terzi, salvo che lo richieda il diritto dell'Unione o nazionale, e in tal caso informa il Titolare prima del trattamento, ove non vietato. Le istruzioni iniziali sono raccolte nell'Allegato IV; istruzioni ulteriori sono impartite per iscritto, anche via e-mail, ai recapiti indicati in intestazione.

Camelot informa il Titolare senza ingiustificato ritardo e, ove possibile, entro 5 giorni lavorativi dal momento in cui viene a conoscenza del fatto che un'istruzione può violare il GDPR o altra disposizione in materia. Restano a carico del Titolare le conseguenze derivanti da istruzioni illegittime, incomplete o tardive, salvo il caso in cui Camelot abbia eseguito l'istruzione pur essendo manifesta la violazione. Camelot non tratta i dati per finalità proprie.

4 Art. 4, persone autorizzate e riservatezza

Camelot garantisce che le persone autorizzate al trattamento si sono impegnate alla riservatezza o hanno un adeguato obbligo legale di riservatezza, sono formate e operano nei limiti dei profili di autorizzazione assegnati. Gli amministratori di sistema sono individuati, designati e verificati in conformità al provvedimento del Garante del 27 novembre 2008 e successive integrazioni, e i loro accessi sono registrati.

5 Art. 5, misure di sicurezza

Camelot mette in atto le misure tecniche e organizzative di cui all'art. 32 GDPR descritte nell'Allegato II, tenendo conto della natura del trattamento e dei rischi per i diritti e le libertà degli interessati, incluse la segretezza dello scrutinio e l'integrità degli esiti richieste dall'Allegato tecnico MIM. Le misure possono essere aggiornate in senso migliorativo o equivalente senza riduzione del livello complessivo di protezione.

Le misure di cui all'Allegato II presidiano l'infrastruttura e la piattaforma di competenza di Camelot. Restano a carico del Titolare:

- la sicurezza dei dispositivi e delle reti utilizzati dagli interessati e dalle persone autorizzate;
- la custodia delle credenziali di accesso;
- la corretta configurazione dei ruoli e del registro degli aventi diritto;
- la gestione della piattaforma di videoconferenza eventualmente scelta dall'Istituzione, ad esempio Google Meet.

6 Art. 6, sub-responsabili

Il Titolare autorizza in via generale il ricorso ai sub-responsabili elencati nell'Allegato III. Camelot informa il Titolare di ogni modifica prevista, aggiunta o sostituzione, con preavviso di almeno 15 giorni, dando al Titolare la possibilità di opporsi per motivi legittimi e documentati. In caso di opposizione e in mancanza di soluzione alternativa, il Titolare può recedere dal Contratto limitatamente al servizio interessato.

L'elenco aggiornato dei sub-responsabili autorizzati, con ruolo, localizzazione e garanzie, è pubblicato e mantenuto aggiornato alla pagina www.camelot.vote/scuole/kit-conformita, che costituisce parte integrante dell'Allegato III. Le aggiunte o sostituzioni sono pubblicate sulla pagina e comunicate al Titolare, con preavviso di 15 giorni, all'indirizzo email indicato in contratto; in mancanza di opposizione motivata entro tale termine la modifica si intende accettata.

Camelot impone a ciascun sub-responsabile, mediante contratto, gli stessi obblighi in materia di protezione dei dati contenuti nel presente accordo e resta interamente responsabile verso il Titolare dell'adempimento degli obblighi del sub-responsabile, ai sensi dell'art. 28, par. 4, GDPR.

7 Art. 7, assistenza al Titolare e diritti degli interessati

Tenendo conto della natura del trattamento, Camelot assiste il Titolare con misure tecniche e organizzative adeguate al fine di dare seguito alle richieste di esercizio dei diritti di cui al Capo III del GDPR. Le richieste eventualmente ricevute da Camelot sono trasmesse al Titolare senza ingiustificato ritardo e comunque entro 5 giorni lavorativi, e Camelot fornisce le informazioni e le funzionalità necessarie al riscontro, cioè accesso, esportazione, rettifica, cancellazione e limitazione.

Camelot assiste inoltre il Titolare nel garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 GDPR, mettendo a disposizione la documentazione tecnica, la scheda di supporto alla DPIA e ogni ulteriore informazione ragionevolmente necessaria, anche ai fini dell'eventuale consultazione preventiva del Garante.

8 Art. 8, violazioni dei dati personali

Camelot notifica al Titolare ogni violazione dei dati personali di cui venga a conoscenza senza ingiustificato ritardo e comunque entro 48 ore, all'indirizzo indicato dal Titolare, fornendo le informazioni di cui all'art. 33, par. 3, GDPR nella misura in cui siano disponibili, cioè natura della violazione, categorie e numero approssimativo di interessati e registrazioni coinvolti, probabili conseguenze, misure adottate o proposte, e integrandole man mano.

Camelot documenta la violazione nel proprio registro, collabora alle valutazioni del Titolare ai fini degli artt. 33 e 34 GDPR e adotta le misure di contenimento e rimedio di propria competenza. La notifica al Garante e l'eventuale comunicazione agli interessati restano atti del Titolare.

Gli obblighi di notifica di cui al presente articolo si applicano alle violazioni che coinvolgono i sistemi e i servizi gestiti da Camelot. Restano esclusi gli eventi derivanti da credenziali compromesse del Titolare, dispositivi degli interessati, piattaforme di videoconferenza di terze parti o errata configurazione a cura del Titolare, per i quali Camelot fornisce comunque ragionevole supporto tecnico se richiesta. La valutazione circa l'obbligo di notifica al Garante e di comunicazione agli interessati ai sensi degli artt. 33 e 34 GDPR resta di esclusiva competenza del Titolare.

9 Art. 9, trasferimenti verso Paesi terzi

Il trattamento è eseguito in via principale in data center ubicati nell'Unione Europea. Il servizio di monitoraggio degli errori applicativi tratta i dati in Germania. Eventuali trasferimenti verso Paesi terzi connessi a servizi accessori, indicati nell'Allegato III, avvengono esclusivamente in presenza delle garanzie di cui al Capo V del GDPR, cioè decisione di adeguatezza della Commissione europea ovvero clausole contrattuali tipo, con le misure supplementari eventualmente necessarie.

10 Art. 10, audit e ispezioni

Camelot mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR, incluse certificazioni, documentazione tecnica e sintesi degli esiti delle verifiche di sicurezza periodiche, e consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da altro soggetto da questi incaricato.

Salvo violazioni o eventi che giustificano verifiche straordinarie, gli audit sono svolti con preavviso scritto di almeno 15 giorni lavorativi, al massimo una volta l'anno, in orario lavorativo, con modalità che non compromettano la sicurezza del servizio né la riservatezza dei dati di altri clienti, e a costi a carico del Titolare.

Prima di procedere a un'ispezione in loco, il Titolare valuta se le proprie esigenze possano essere soddisfatte mediante questionari, certificazioni, report di audit indipendenti o documentazione tecnica aggiornata. L'ispezione in loco è consentita solo qualora tali strumenti non siano sufficienti e, comunque, nel rispetto delle modalità indicate. Camelot può fornire, in alternativa o integrazione, attestazioni di conformità, esiti di test effettuati o certificazioni ISO e SaaS ACN.

11 Art. 11, restituzione e cancellazione

Per tutta la durata del Servizio il Titolare può esportare in autonomia dati, esiti, verbali e report in formati standard. Al termine del rapporto contrattuale, per qualsiasi causa intervenuto:

- su richiesta del Titolare, formulata entro il periodo di grazia di cui alla lettera successiva, Camelot restituisce i dati personali in un formato strutturato di uso comune entro 30 giorni dalla richiesta;
- in ogni caso, Camelot cancella i dati e le copie esistenti decorso il periodo di grazia di 30 giorni dal termine, fatta salva la conclusione delle operazioni di restituzione in corso e salvi gli obblighi di conservazione previsti dal diritto dell'Unione o nazionale.

Su richiesta, Camelot attesta per iscritto l'avvenuta cancellazione. Restano presso il Titolare i verbali e le evidenze già acquisiti agli atti, la cui conservazione documentale è di competenza dell'Istituzione.

La cancellazione avviene secondo le procedure tecniche di Camelot e può non riguardare immediatamente le copie di backup automatiche, che saranno sovrascritte o eliminate secondo i normali cicli di sicurezza e comunque non oltre 180 giorni dal termine del rapporto. Camelot può conservare dati o documenti per il periodo strettamente necessario all'adempimento di obblighi di legge o alla difesa in giudizio, mantenendoli riservati e limitandone l'accesso.

12 Art. 12, responsabilità e disposizioni finali

Ciascuna Parte risponde dei danni cagionati dal trattamento in conformità all'art. 82 GDPR. Nei rapporti interni, il Titolare manleva e tiene indenne Camelot da ogni pretesa, danno, sanzione o costo derivante da istruzioni illegittime o incomplete, dati inesatti, non aggiornati o trattati in assenza di base giuridica, mancata o incompleta informativa, errata configurazione della piattaforma o del registro degli aventi diritto, violazione degli obblighi di custodia delle credenziali.

Camelot manleva il Titolare per i danni direttamente derivanti dalla violazione degli obblighi posti a proprio carico dal presente accordo o dall'art. 28 GDPR, qualora tali danni siano imputabili a dolo o colpa grave di Camelot. In ogni caso, la responsabilità complessiva di Camelot per danni indiretti o perdita di profitto resta esclusa nei limiti consentiti dalla normativa applicabile, fermi i diritti degli interessati ai sensi dell'art. 82 GDPR.

Camelot tiene il registro delle categorie di attività di trattamento svolte per conto del Titolare, ai sensi dell'art. 30, par. 2, GDPR, e coopera, su richiesta, con l'autorità di controllo. Il presente accordo ha la stessa durata del Contratto e resta efficace fino al completamento delle operazioni di cui all'art. 11. Per quanto non previsto si applicano il GDPR, il D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018, e il Contratto in essere tra le parti.

Foro competente. Per ogni controversia derivante dal presente accordo sarà competente in via esclusiva il Foro di Torino, salvo il diverso foro inderogabile previsto a tutela del consumatore o dell'interessato.

CAMPI

Luogo e data [_____]

IL TITOLARE

L'istituzione scolastica, il Dirigente scolastico pro tempore

Firma, anche digitale

IL RESPONSABILE

Camelot S.r.l. SB, il legale rappresentante pro tempore

Firma, anche digitale

ALLEGATO I

Descrizione del trattamento

TABELLA

ELEMENTO	CONTENUTO
Oggetto	Erogazione delle piattaforme Camelot Voto e Camelot Assemblee per la gestione digitale delle sedute degli organi collegiali e delle operazioni di voto dell'Istituzione, cioè sedute deliberative a distanza o miste ed elezioni telematiche ove deliberate dall'Istituzione.
Durata	Pari alla durata del Contratto, oltre ai termini di restituzione e cancellazione di cui all'art. 11 dell'accordo.
Natura e operazioni	Trattamento automatizzato. Raccolta e registrazione del registro degli aventi diritto caricato dal Titolare; invio delle convocazioni e dei collegamenti personali; autenticazione; rilevazione di presenze e quorum; raccolta e conteggio delle espressioni di voto; produzione di verbali, esiti e report; conservazione ed esportazione; cancellazione.
Finalità	Consentire all'Istituzione lo svolgimento a distanza delle attività collegiali a carattere deliberativo di cui all'art. 44, comma 3, lett. a) e b), del CCNL Istruzione e Ricerca 2019-2021, in conformità alla nota MIM prot. 3803 del 30 giugno 2026, nonché delle elezioni telematiche disciplinate dal regolamento d'istituto (D.Lgs. 297/1994, O.M. 215/1991).
Categorie di interessati	Personale docente e dirigente; personale ATA ove componente degli organi; genitori ed esercenti la responsabilità genitoriale; studenti, anche minorenni, ove elettori o componenti; candidati ed eletti; utenti con ruoli di conduzione (presidente, segretario, assistenti).
Categorie di dati	Dati comuni: anagrafici essenziali, recapiti (e-mail istituzionale e numero di cellulare nella versione Premium con OTP via SMS), categoria e ruolo, dati di partecipazione (presenze, orari, interventi), espressioni di voto palese, dato di avvenuto voto, log tecnici, flussi audio-video delle sedute ove attivati. Nel voto a scrutinio segreto la preferenza è anonimizzata in modo irreversibile e non è riconducibile al votante. Eventuali dati ex art. 9 GDPR possono emergere unicamente dal contenuto di singole deliberazioni palesi.
Conservazione	Per la durata del Servizio. Al termine, restituzione su richiesta e cancellazione decorsi 30 giorni (art. 11). I verbali e le evidenze acquisiti agli atti dell'Istituzione seguono i tempi di conservazione documentale del Titolare.

NOTA

Il Titolare può integrare o restringere le voci del presente allegato in base alla configurazione effettivamente adottata, dandone atto per iscritto. In assenza di integrazioni si applica la descrizione qui riportata.

II

ALLEGATO II

Misure tecniche e organizzative, art. 32 GDPR

Le misure sono descritte per esteso nella Documentazione tecnica di rispondenza all'Allegato tecnico MIM, che integra il presente allegato.

1. Identificazione, autenticazione e controllo degli accessi

- Identità individuali univoche e non condivise, associate al singolo avente diritto tramite collegamento personale e univoco e verificate rispetto al registro degli aventi diritto, con blocco dell'uso condiviso o impersonale delle credenziali.
- Autenticazione calibrata sul rischio. Nella versione Premium, secondo fattore OTP usa e getta via SMS e autenticazione forte tramite SPID, CIE o CNS, con integrazione Single Sign-On ove configurata.
- Controllo degli accessi basato sui ruoli, cioè Presidente, Segretario, Assistente, Votante e Ospite, secondo il principio del minimo privilegio, con distinzione tra controllo di identità e controllo di autorizzazione (ruolo, platea, finestra temporale).
- Gestione sicura delle sessioni: durata limitata, interruzione automatica alla scadenza, revoca dei token abilitata, 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.

2. Integrità e univocità del voto, segretezza dello scrutinio

- Un solo voto per avente diritto e per quesito, controllo di univocità su registro separato dall'archivio delle preferenze, validazione delle espressioni alla ricezione, conteggio automatico senza spoglio, quesito chiuso non riapribile, con ripetizione affidata a una nuova votazione tracciata.
- Voto segreto, con cifratura della preferenza sul dispositivo del votante prima della trasmissione, separazione strutturale e irreversibile tra autenticazione ed espressione, nessun archivio della corrispondenza tra identità e voto, log e metadati gestiti in modo da impedire la re-identificazione anche indiretta, verificabilità dell'esito complessivo senza compromissione delle singole preferenze.

3. Sicurezza applicativa e di rete

- Comunicazioni cifrate con HTTPS e TLS e certificati gestiti, cifratura dei dati e dei backup a riposo, gestione delle chiavi tramite servizio dedicato.
- Segregazione delle reti, con account AWS separati per ambiente, e degli ambienti di sviluppo, collaudo e produzione, senza dati di produzione negli ambienti di sviluppo.
- Gestione delle vulnerabilità, con aggiornamenti periodici, vulnerability assessment e penetration test periodici e presa in carico dei rilievi.

4. Continuità operativa e disaster recovery

- Tabelle dati replicate in modo asincrono su quattro regioni AWS dell'Unione Europea (Francoforte, Irlanda, Parigi, Stoccolma) e servizi applicativi distribuiti su più regioni; ripristino point-in-time sulla maggior parte delle tabelle di produzione e backup giornalieri cifrati degli archivi di voto conservati 35 giorni; procedure di ripristino nell'ambito del SGSI.

5. Registrazione, monitoraggio e amministratori di sistema

- Registrazione degli eventi rilevanti della seduta, cioè apertura e chiusura delle votazioni, pause e riprese, esiti, e delle operazioni rilevanti degli utenti. Registrazione e monitoraggio degli accessi, inclusi quelli amministrativi, e monitoraggio dell'infrastruttura con allarmi.
- Amministratori di sistema individuati, designati per iscritto e verificati annualmente ai sensi del provvedimento del Garante del 27 novembre 2008 e successivi, con registrazione dei log riguardanti gli accessi amministrativi.

6. Verbali, evidenze e servizi fiduciari

- Verbale costruito durante i lavori e finalizzato in forma immodificabile con impronta digitale del documento. Esportazione di verbali, esiti e report in formati standard, PDF ed Excel, con i metadati a corredo, e registro eventi della seduta con data e ora.
- Firma digitale e marcatura temporale di verbali e report a cura dell'Istituzione, con assistenza di Camelot; su richiesta, tramite InfoCert S.p.A.

7. Misure organizzative e certificazioni

- Sistema di Gestione per la Sicurezza delle Informazioni certificato EN ISO/IEC 27001:2022 con estensioni cloud ISO/IEC 27017:2015 e ISO/IEC 27018:2019, sistema qualità EN ISO 9001:2015, servizio SaaS qualificato sul Cloud Marketplace ACN, livello QC1, scheda SA-7041.
- Designazione e formazione delle persone autorizzate, istruzioni operative, procedura di gestione delle violazioni secondo la Data Breach Policy di Camelot, con registro, canale dedicato privacy@camelot.vote, procedura di gestione dei malfunzionamenti con sospensione ed eventuale ripetizione delle operazioni di voto, tracciate a fini di verbalizzazione.
- Data center ubicati nell'Unione Europea, residenza dei dati nell'Unione per i servizi principali, verifica periodica dei sub-responsabili.



ALLEGATO III

Sub-responsabili autorizzati

L'elenco aggiornato dei sub-responsabili autorizzati, con ruolo, localizzazione e garanzie, è pubblicato e mantenuto aggiornato alla pagina www.camelot.vote/scuole/kit-conformita, che costituisce parte integrante dell'Allegato III. Le aggiunte o sostituzioni sono pubblicate sulla pagina e comunicate al Titolare secondo l'art. 6 dell'accordo. Non sono coinvolti nel Servizio ulteriori fornitori con accesso ai dati personali del Titolare.

TABELLA

SUB-RESPONSABILE	ATTIVITÀ	LUOGO DEL TRATTAMENTO E GARANZIE
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Lussemburgo	Infrastruttura cloud (elaborazione, database, archiviazione, backup, rete e sicurezza perimetrale).	Data center nell'Unione Europea, regione principale Francoforte (eu-central-1), repliche Irlanda (eu-west-1), Parigi (eu-west-3) e Stoccolma (eu-north-1). Impegno contrattuale al mantenimento dei dati nelle regioni UE selezionate.
Sentry	Monitoraggio tecnico degli errori applicativi.	Trattamento nell'Unione Europea (Germania).
LiveKit, Inc., Stati Uniti	Servizi di streaming audio-video per le sedute in diretta (Camelot Assembly), ove attivati.	Trasferimento assistito dalle garanzie del Capo V GDPR (clausole contrattuali tipo e, ove applicabile, decisione di adeguatezza EU-USA), con misure supplementari. Flussi multimediali di seduta, senza accesso ai dati di voto. Azienda aderente al EU-USA Data Privacy Framework, www.dataprivacyframework.gov/list
Twilio Inc., Stati Uniti	Fornitore di recapito SMS, invio degli OTP via SMS nella versione Premium, ove attivata.	Trattamento limitato a numero di cellulare e contenuto del messaggio di servizio. Trasferimento assistito dalle garanzie del Capo V GDPR (clausole contrattuali tipo e, ove applicabile, decisione di adeguatezza EU-USA). Azienda aderente al EU-USA Data Privacy Framework, www.dataprivacyframework.gov/list
InfoCert S.p.A., Italia	Gateway di identità SPID, CIE e CNS e, su richiesta, firma digitale e marcatura temporale di verbali e report, ove attivate.	Trattamento in Italia e nell'Unione Europea, limitato ai dati necessari all'autenticazione e all'apposizione di firma e marca temporale.
Openapi S.p.A., Italia	Recapito PEC, ove attivato.	Trattamento in Italia.

Videoconferenza dell'Istituzione

Ove la seduta si svolga sulla piattaforma di videoconferenza già in uso all'Istituzione, ad esempio Google Meet, anche tramite il componente aggiuntivo Camelot, il trattamento dei flussi audio-video avviene nell'ambito del rapporto già in essere tra l'Istituzione e il relativo fornitore, ad esempio il contratto Google Workspace for Education, e resta fuori dal perimetro del presente accordo. Camelot tratta in tal caso i soli dati di presenza, quorum e voto.

Opposizione del Titolare

Qualora il Titolare si opponga all'aggiunta o sostituzione di un sub-responsabile per motivi non ragionevoli o senza indicare una soluzione alternativa compatibile con il Servizio, Camelot non sarà responsabile per eventuali ritardi o impossibilità di erogazione del servizio interessato. Il recesso parziale di cui all'art. 6 non darà diritto a rimborsi o indennizzi ove l'impossibilità dipenda da opposizione infondata.

NOTA

I trasferimenti verso Paesi terzi eventualmente connessi ai servizi accessori qui richiamati sono regolati dall'art. 9 dell'accordo.

IV

ALLEGATO IV

Istruzioni documentate del Titolare

1. Trattare i dati personali esclusivamente per l'erogazione del Servizio, nei limiti dell'Allegato I, e non per finalità proprie o di terzi. Nessun uso commerciale, statistico o di profilazione.
2. Applicare e mantenere le misure di sicurezza dell'Allegato II, garantendo in particolare la segretezza dello scrutinio segreto, l'univocità e l'integrità del voto e l'immodificabilità del verbale finalizzato.
3. Non conservare, in alcun archivio o log, la corrispondenza tra identità del votante e preferenza espressa a scrutinio segreto, e gestire log e metadati in modo da escludere la re-identificazione anche indiretta.
4. Consentire l'accesso ai dati alle sole persone autorizzate e agli amministratori di sistema designati, nei limiti dei rispettivi profili, e non comunicare dati a terzi salvo istruzione scritta del Titolare o obbligo di legge.
5. Trasmettere al Titolare, entro 5 giorni lavorativi, ogni richiesta degli interessati e ogni istanza dell'autorità di controllo ricevute in relazione al Servizio, fornendo assistenza per il riscontro.
6. Notificare le violazioni dei dati personali secondo l'art. 8 dell'accordo, senza ingiustificato ritardo e comunque entro 48 ore, all'indirizzo e-mail o PEC comunicato dall'Istituzione per le notifiche.
7. Non trasferire dati verso Paesi terzi al di fuori dei casi di cui all'Allegato III senza previa autorizzazione scritta del Titolare e comunque nel rispetto del Capo V GDPR.
8. Al termine del rapporto, restituire e cancellare i dati secondo l'art. 11 dell'accordo, attestando per iscritto l'avvenuta cancellazione su richiesta.
9. Comunicare tempestivamente ogni variazione sostanziale del Servizio, delle misure di sicurezza o dei sub-responsabili che incida sulla conformità dichiarata, aggiornando la documentazione tecnica a corredo.
10. Supportare il Titolare nella valutazione d'impatto sulla protezione dei dati e nelle eventuali interlocuzioni con il Garante, mettendo a disposizione la scheda di supporto DPIA e la documentazione tecnica.

NOTA

Le istruzioni sono normalmente impartite dal Titolare al Responsabile per iscritto, anche mediante e-mail o PEC ai recapiti indicati. In caso di istruzioni ambigue, incomplete o potenzialmente non conformi, Camelot può richiedere chiarimenti e, nel frattempo, sospendere le operazioni interessate senza che ciò costituisca inadempimento. Le istruzioni orali o telefoniche devono essere confermate per iscritto entro 3 giorni lavorativi.

CONTATTI E DOCUMENTAZIONE

Il canale privacy è dedicato, e la documentazione tecnica accompagna l'accordo

Per l'esercizio dei diritti degli interessati, per le richieste di audit, per l'elenco aggiornato dei sub-responsabili e per la scheda di supporto alla DPIA il riferimento è privacy@camelot.vote. La Documentazione tecnica di rispondenza all'Allegato tecnico MIM e la dichiarazione di conformità integrano l'Allegato II del presente accordo.

Privacy e diritti degli interessati
privacy@camelot.vote

Sito
camelot.vote

Informazioni sul servizio
info@camelot.vote

Sede
Via Palestro 62, 10015 Ivrea (TO)