Specifiche tecniche sistema di voto online ELIGO – versione per elezioni INPGI 2020

Documentazione Tecnica

Sommario

1 Introduzione

1.1 Oggetto e scopo

Il presente documento descrive le caratteristiche tecniche adottate dal sistema di voto online ELIGO (v.5.1 rilasciato ad ottobre 2019) nella versione utilizzata per le elezioni INPGI 2020.

2 Caratteristiche tecniche della soluzione

2.1 Generalità

La soluzione offerta da ID Technology è relativa alla licenza d'uso della piattaforma di voto **ELIGO** in **cloud computing**, rilasciato sui sistemi cloud del nostro fornitore di servizi Aruba S.p.A.

La piattaforma **ELIGO** è frutto della pluriennale esperienza di ID Technology nel campo del voto via internet ed è stato ampiamente e ripetutamente utilizzato da Enti ed Associazioni ed anche l'Università di Torino, l'Università di Bologna, l'Università di Udine e l'Università di Napoli.

Il servizio di voto **ELIGO** è stato verificato dall'ente "**Garante per la protezione dei dati**" riguardante la conformità del Servizio alla disciplina, di cui al D.lg. n.196/2003, relativa ai trattamenti dei dati personali ed alla sicurezza e anonimato del voto, che l'ha ritenuto conforme alla normativa sia per quanto attiene il processo di trattamento dei dati sia per la segretezza delle preferenze espresse durante le votazioni.

Anche il Tribunale Ordinario di Roma si è espresso in merito.
La Sentenza del Tribunale Ordinario di Roma elimina qualsiasi possibilità di contestazione del voto online.
Secondo la sentenza del tribunale, infatti, con l'adozione della piattaforma di voto online **ELIGO** "risultano approntate una serie di cautele tecnologiche idonee ad impedire un uso scorretto o improprio del voto e ad offrire le maggiori garanzie di riservatezza, segretezza e libertà di espressione del voto".
La sentenza del tribunale ha avuto una tale rilevanza da essere riportata dal quotidiano economico, giuridico e politico ItaliaOggi, che ha sottolineato come **ELIGO** garantisca "la massima partecipazione democratica e, con un sistema più sicuro e più protetto, assicura un risparmio economico".

Con il servizio **ELIGO** di ID Technology, i nostri clienti possono affrontare l'introduzione del voto telematico in "outsourcing" in piena tranquillità, potendo contare sull'expertise del nostro team di prodotto e sulla affidabilità del software applicativo che eroga le funzionalità di generazione credenziali e di voto, delle procedure di gestione del voto e dell'addestramento del personale, già sperimentata da oltre 2.000.000 elettori.

2.2 Fornitore dei servizi cloud ospitanti il servizio di voto

ID Technology si appoggia da diversi anni sui servizi cloud offerti da un service provider totalmente italiano, ARUBA S.p.a., dove rilasciamo e configuriamo l'infrastruttura utile a garantire il corretto funzionamento del sistema di voto ELIGO utilizzando il servizio Private Cloud offerto in modalità Iaas.

In qualità di fornitore di servizi cloud, Aruba S.p.a. è dotata delle seguenti certificazioni:

- ISO 9001:2015,
- ISO 27001:2013,
- Cloud della PS / CSP qualificato,
- Dichiarazione di conformità ISO 27018:2014,
- Dichiarazione di conformità ISO 27017:2015,
- Dichiarazione di conformità ISO 27035:2016,
- ISO 14001:2015,
- ISO 50001:2011,
- Certificazione ANSI/TIA 942-B-2017,
- Certificazione ISAE 3402:2011 Type II Report,
- CISPE Service Declared - Servizi aderenti al Codice di Condotta CISPE per la protezione dei dati

Il Global Cloud Data Center di Aruba, dove verranno attivati i servizi offerti, è un data center campus di 200.000 m² a Ponte San Pietro (BG), raggiungibile in pochi minuti da Milano. Tutti gli impianti sono stati progettati e costruiti per soddisfare ed eccedere i massimi livelli di resilienza previsti dal livello Rating 4 (former Tier 4) di ANSI/TIA 942-B-2017. All'interno del Data Center IT3 è possibile scambiare traffico con tutti gli operatori presenti al Milan Internet eXchange di Milano, grazie al Point of Presence di MIX.
Il Campus tecnologico è di 200.000 m² con 90.000 m² di superficie coperta destinata a data center dove vengono offerti massimi livelli di sicurezza logica e fisica con vigilanza armata 24/7/365 e 7 diversi perimetri di controllo.
Sono disponibili fino a 90 MW di potenza, con produzione autonoma di energia idroelettrica e fotovoltaica, doppio power center multi-modulare con UPS a ridondanza 2N + 1, potenza personalizzabile fino a 40 kW per rack, generatori di emergenza ridondati con autonomia a pieno carico di 48 ore senza rifornimento, Data hall composta integralmente di muri tagliafuoco e tetto con doppia copertura isolante, Data Center carrier neutral con disponibilità di connettività gestita.

Il Private Cloud di Aruba Cloud è un servizio IaaS, che permette di creare Virtual Data Center contenenti server virtuali, firewall e reti, con possibilità di espansione o riduzione a seconda delle diverse esigenze del cliente. Il Private Cloud consente di possedere sia risorse computazionali, sia risorse di rete ad uso esclusivo.
Tutta l'infrastruttura è in alta affidabilità e resiliente ai guasti. L'intera struttura Private Cloud si appoggia su una solida componente di networking ridondata, interamente a 10 Gbit/sec. L'hardware impiegato per l'erogazione del servizio è dotato di ridondanza e lo storage è replicato.
Il servizio Private Cloud permette di acquistare quantità variabili di risorse computazionali (vCPU, RAM e HD), di rete (Virtual Lan, Firewall e IP pubblici) e servizi aggiuntiivi (Cloud DRaaS e Cloud Bare Metal Backup) da utilizzare tramite la console web VMware vCloud Director, per poter creare e gestire in completa autonomia data center Virtuali completi di funzionalità evolute come Firewall perimetrali, Bilanciatori e concentratori VPN.

Il servizio è pensato nell'ottica delle massime prestazioni: Rete interamente a 10 Gbit/sec, Server con processori ad elevatissima frequenza e di ultima generazione, Storage ridondato e replicato in modalità sincrona su di un data center secondario sono caratteristiche uniche che sono pensate per le aziende più esigenti.

Aruba eroga delle risorse computazionali che saranno poi utilizzate dal cliente secondo le proprie esigenze in maniera autonoma ed in totale sicurezza.

Questa soluzione ci consente di offrire ad INPGI il sistema di voto ELIGO con prestazioni adattabili alla numerosità e contemporaneità degli elettori.

Aruba Cloud Computing viene erogato tramite i Data Center del Gruppo e definisce i parametri di riferimento per l'erogazione del servizio (SLA) con un Uptime del 99,95% così definito:

- Uptime del 99,95% su base annuale, per la disponibilità dei nodi fisici (server) che ospitano l'Infrastruttura virtuale; per il servizio Cloud Server Smart l'uptime è del 99,80% su base annua
- Uptime del 99,95% su base annuale, di accessibilità tramite rete internet alla Infrastruttura virtuale creata ed allocata dal Cliente; per il servizio Cloud Server Smart l'uptime è del 99,80% su base annua
- Uptime del 100% su base annuale per fornitura di elettricità e/o aria condizionata

L'accesso alle macchine virtuali ospitanti i servizi di voto è consentito esclusivamente al personale ID Technology nominato ed autorizzato ad avvio progetto secondo i dettami GDPR, previa installazione e configurazione di apposita connessione VPN, necessaria ad impedire ogni tentativo esterno non autorizzato di accesso alle macchine.

Tutte le porte TCP/UDP in entrata/uscita sui servers saranno bloccate dal firewall hardware in dotazione (rimangono aperte esclusivamente le porte necessarie per la comunicazione web applicativa [http/https] e la porta necessaria all'inoltro e-mail).

L'intera infrastruttura cloud è protetta attraverso l'adozione di un firewall Fortigate VM-00, Software, Forticare e UTM di ultima generazione in grado di prevenire ed impedire attacchi malevoli ai sistemi.

Le credenziali di accesso alla VPN, ai servers, all'interfaccia amministrativa del voto saranno a conoscenza esclusiva del personale tecnico specialista di prodotto, nominati dal referente tecnico ID Technology assegnato al processo.

Il Private Cloud di Aruba Cloud è un servizio IaaS, che permette di creare Virtual Data Center contenenti server virtuali, firewall e reti, con possibilità di espansione o riduzione a seconda delle diverse esigenze del cliente.

Il servizio Aruba Private Cloud è certificato AgID e disponibile anche per Pubbliche Amministrazioni e/o operatori che forniscono risorse alla Pubblica Amministrazione per l'erogazione dei propri servizi.
In quanto Cloud Service Provider qualificato di tipo C, infatti, Aruba offre soluzioni IaaS e Saas in linea con l'obbligo previsto dal 1° aprile 2019 secondo il quale le Pubbliche Amministrazioni possono utilizzare esclusivamente servizi Cloud erogati da Cloud Service Provider qualificati e presenti nel marketplace ufficiale dell'Agenzia per l'Italia Digitale.

Aruba è certificata ISO 27001 garantendo il rispetto di determinati standard di sicurezza nella gestione dei dati e delle informazioni aziendali, preservandone l'integrità, la riservatezza e la disponibilità.

I nostri servizi erogati su tale infrastruttura sono così articolati in un'ottica di sicurezza e compliance GDPR:

1. Storage ridondato e replicato
   Block storage ridondato su disco SSD con replica su data center diversi nello stesso paese (Italia e Francia) o in paesi diversi (Polonia e Repubblica Ceca).
   (Approfondimenti: GDPR – art. 32, comma 1, par. b)

2. Network ridondato
   L'infrastruttura di rete è completamente ridondata per garantire il funzionamento della rete in caso di guasto.
   Il data center dove saranno rilasciati i servizi di voto è certificato ai massimi livelli per la resilienza e qualità infrastrutturale previsti dalla normativa ANSI/TIA 942 e certificati Rating 4.
   (Approfondimenti: GDPR – Art. 32, comma 1, par. b)

3. Snapshot del server virtuale
   Possibilità di creare copie della macchina virtuale in un dato punto temporale.
   (Approfondimenti: GDPR – Art. 32, comma 1, par. c)

4. Conforme al codice CISPE
   Il marchio di garanzia sancisce la conformità al Codice di Condotta CISPE e garantisce la libertà di archiviare ed elaborare i dati all'interno dello Spazio Economico Europeo.
   (Approfondimenti: GDPR – Art. 40)

5. Two factor authentications
   L'accesso al Pannello di Controllo dell'intera infrastruttura avviene tramite un doppio sistema di autenticazione.
   (Approfondimenti: GDPR – art. 32, comma 2)

6. DRaaS disponibile
   Disaster Recovery as a Service adottato per consentire la creazione di repliche di dati nel Private Cloud di Aruba, sfruttando il software Zerto.
   (Approfondimenti: GDPR – Art. 32)

I dati conservati all'interno della infrastruttura sono sotto il totale controllo di ID Technology. Aruba non può accedere ed utilizzare in qualsiasi modo i dati collocati sul cloud. Tutto ciò è garantito e certificato da Aruba nel rispetto del Codice di Condotta CISPE.

Tutti i dati sono gestiti in conformità alla normativa sulla privacy ed in particolare al recente regolamento UE 2016/679 (GDPR). ID Technology agisce in qualità di incaricato esterno del trattamento dati esclusivamente ai fini della conduzione di servizi di voto.
Il personale tecnico è stato opportunamente formato e sono stati definiti i processi di trattamento dei dati personali nonché i criteri di cancellazione degli stessi successivamente alla conclusione del processo elettorale.

2.3 Componenti hardware e software utilizzati per il rilascio del servizio di voto in cloud

Il sistema di voto online ELIGO è sviluppato e compilato con tecnologia Microsoft ASP.NET su piattaforma Windows server 2012 R2, mentre la base dati relazionale utilizzata per l'archiviazione dei dati è Microsoft Sql Server 2016 R2 nella versione Enterprise Edition.

Il rilascio in cloud del servizio prevede che possano essere utilizzate risorse hardware a complessità crescente, studiate sulla base delle specifiche esigenze che il cliente intende dotarsi in materia di sicurezza ed affidabilità.

La configurazione scelta per le lezioni INPGI prevede l'utilizzo di 3 server:
Un server utile ad ospitare la cabina elettorale esposta in rete per il periodo previsto per il voto on-line
Due server ospitanti le diverse basi dati relazionali sottostanti il servizio di voto, in ambiente SLQ Server 2016 Enteprise in configurazione di mirroring per la gestione di fault tolerance, non esposte in rete.

Su questa configurazione i dati contenuti nella base dati di appoggio vengono automaticamente sottoposti a backup protetto ogni ora. Questa configurazione, adottata fino ad oggi da tutti i nostri clienti che abbiano acquistato il servizio di voto nella sua forma standard, supporta senza esitazioni notevoli volumi in termini di utenze concorrenti collegate per votare.

2.3.1 Protezione tramite firewall hardware

E nativamente offerta la protezione dell'intera infrastruttura contenente i sistemi informativi sottostanti il servizio di voto, tramite l'adozione un **firewall fortigate** VM-00 UTM, FORTICARE fornito dal nostro service provider Aruba.
In questo modo siamo in grado di aumentare notevolmente la sicurezza dei sistemi esposti in rete, garantendo la totale chiusura delle porte tcp/udp ad esclusione delle porte 80 e 443 utili all'accesso web del sistema di voto.

2.3.2 Protezione tramite Virtual Private Network (VPN)

Per aumentare i livelli di sicurezza dei sistemi ospitanti il servizio di voto, viene sempre installata e configurata una rete privata VPN (controllata tramite il firewall Fortigate) su ognuno dei servers facenti parte del servizio di voto.
In questo modo l'accesso remoto ai sistemi è consentito esclusivamente al nostro personale qualificato dotato di opportuno client VPN e relative credenziali per l'accesso.
L'accesso in desktop remoto non consentito fuori dal perimetro della VPN perché bloccato a monte dal firewall hardware.

2.3.3 Sicurezza fisica, logica ed applicativa

La sicurezza fisica (controllo accessi, continuità elettrica, antincendio) è garantita dal provider del servizio di cloud computing, che ha in carico anche la fornitura della banda di connessione e la sicurezza logica di accesso (firewall, antivirus perimetrali, log di connessione, monitoraggio).
Per quanto riguarda la sicurezza applicativa, **ELIGO** è stato progettato e realizzato da ID Technology in modo da aggiungere, alla sicurezza fisica e logica offerta dal contesto, ulteriori livelli di sicurezza applicativa, tra cui: la generazione casuale dei PIN di accesso inviate per SMS agli elettori, la classificazione degli utenti in profili predefiniti mappati sulle funzionalità dell'applicativo, la completa separazione del dato del voto dal dato del votante e l'utilizzo della **crittografia dei voti** a chiave doppia.
La versione 5.1 di Eligo è frutto di molteplici interventi di manutenzione mirati ad aumentarne il livello di sicurezza e conformità secondo i suggerimenti della fondazione OWASP (The Open Web Application Security Project (OWASP). Nello specifico sono state verificate e rese compliant tutte le funzionalità indicate nel documento https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
Di pari passo sono stati condotti innumerevoli test di penetrazione (test eseguiti sia dal nostro reparto tecnico che da alcune multinazionali nostre clienti), che ci hanno permesso di monitorare e chiudere ogni falla di sicurezza identificata.

Il protocollo di comunicazione web, che permette agli elettori l'utilizzo della cabina di voto, è crittografato tramite connessione cifrata su protocollo https (SSL) mediante certificato digitale a 256 bit o superiore.
Ogni accesso al sistema di voto viene tracciato tramite l'abilitazione dei logs nativi del web server ospitante il servizio di voto ed ulteriormente tracciati in una opportuna tabella applicativa in cui viene registrata ogni operazione eseguita dai votanti; non vengono tracciate le scelte relative alle preferenze indicate nelle relative schede di voto.
Le informazioni tracciate nella tabella di log applicativo sono: indirizzo ip, identificativo dell'elettore, tipologia dell'operazione, operazione eseguita e data.

Il database utilizzato dal servizio di voto per gestire tutte le informazioni sulla votazione ed i relativi voti sottomessi è MS SQL SERVER 2016 R2 nella versione enterprise, configurato per crittografare a livello nativo i dati in esso contenuti (Crittografia TDE).
Su tale base dati sono attivati i transaction logs di sistema, utili a contenere la storia completa delle azioni avvenute sui dati e sulla struttura dei dati.

Ogni transaction log completo conserva in modo IMMODIFICABILE l'elenco di tutti i cambiamenti che avvengono nella base dati (auditing completo) e consente inoltre di garantire l'integrità dei dati riservati memorizzati nel database. Il transaction log può essere consultato per verificare il dettaglio di tutte le operazioni avvenute su tale sistema. La consultazione del transaction log offre indiscutibilmente una modalità di controllo su cosa sia avvenuto sul sistema, chi l'abbia eseguito, quando l'abbia eseguito e cosa sia avvenuto.

Per quanto riguarda la protezione dei dati (TDE) conservati nella base dati sottostante il servizio di voto, SQL server, ci permetterà per le elezioni INPGI di definire regole utili a crittografare automaticamente i dati, così da impedire a seguito di un furto dei files costituenti la base dati di poter estrarre i dati in esso contenuti. Questa modalità di crittografia è chiamata TDE (Transparent Data Encryption), che non richiede alcuna modifica alle applicazioni che accedano al database.

Transparent Data Encryption (TDE) consente di crittografare file di dati di SQL Server con un'operazione nota come crittografia dei dati inattivi. Per proteggere il database è possibile adottare alcune accortezze, tra cui la progettazione di un sistema sicuro, la crittografia dei dati riservati e la compilazione di un firewall attorno ai server di database. Tuttavia, nel caso in cui i supporti fisici (ad esempio unità o nastri di backup) venissero rubati, un malintenzionato potrebbe ripristinare o collegare il database e accedere ai dati. Una soluzione per ovviare al problema consiste nel crittografare i dati sensibili nel database e proteggere con un certificato le chiavi usate per la crittografia. In questo modo si impedisce a chi è sprovvisto delle chiavi di usare i dati; tuttavia, questo tipo di protezione deve essere pianificato in anticipo

2.3.4 Segretezza del voto

Il sistema di voto impedisce la ricostruibilità della relazione tra voto e votante, tale processo è stato verificato dal Garante della Privacy che ne ha validato le modalità.
Non è quindi consentito a nessuno, tantomeno al fornitore del servizio, di ricostruire tale legame.
Il database relazionale dove sono conservati i voti espressi è configurato in modo tale che non sia altresì ricostruibile tale relazione incrociando l'analisi dei logs, dei tempi di espressione del voto e degli elettori con le tabelle contenenti i voti veri e propri.
I voti registrati vengono memorizzati in una base dati specifica, diversa da quella contenente i dati degli elettori, così da garantire una netta separazione del dato di voto da quella del votante. I records contenenti i dati relativi ai voti vengono inseriti da ELIGO nel database relativo in maniera casuale e non sequenziale.
Come ulteriore attestazione di segretezza del voto, i voti vengono memorizzati in maniera crittografata (crittografia asimmetrica a doppia chiave) per impedire la lettura dei voti a votazioni aperte e comunque sul database.
Tali accorgimenti ci consentono di garantire quindi che il voto è assolutamente segreto. Anche a valle dello scrutinio dei risultati i dati di voto rimangono anonimi e crittografati nella base dati.

2.3.5 Rispetto della Privacy

Oltre a impedire la ricostruibilità della relazione tra voto e votante, già verificata dal Garante della Privacy, in **ELIGO** la gestione della privacy si estende anche al provider del cloud computing, scelto sul territorio italiano (o europeo) per evitare ogni potenziale contenzioso legale derivante dall'esportazione fuori dal confine nazionale dei dati personali degli Elettori. (Compliance GDPR)

2.3.6 Modalità di adeguamento al GDPR (Regolamento UE 2016/679)

Richiesta
Descrizione dell'adeguatezza ai Principi applicabili al trattamento di dati personali (Artt. dal 5 al 9)

Testo articolo 5 - http://www.privacy-regulation.eu/it/5.htm
Testo articolo 6 - http://www.privacy-regulation.eu/it/6.htm
Testo articolo 7 – http://www.privacy-regulation.eu/it/7.htm
Testo articolo 8 – http://www.privacy-regulation.eu/it/8.htm

Testo articolo 9 - http://www.privacy-regulation.eu/it/9.htm

Risposta
ART. 5
LICEITÀ, CORRETTEZZA E TRASPARENZA
Il trattamento è relativo esclusivamente alla esecuzione di servizi per votazioni del Titolare dei dati
Il trattamento è disciplinato da uno specifico contratto fra le parti. ID Technology agirà da Responsabile esterno del trattamento.
I dati sono trattati in modo corretto e trasparente.
FINALITÀ
I dati personali sono conferiti e trattati solo al fine di erogazione di un servizio di voto elettronico per le elezioni del Committente.
NECESSITÀ, NON ECCEDENZA, ESSENZIALITÀ
I dati personali conferiti e trattati sono minimi e funzionali alla gestione delle varie fasi di un processo di voto elettronico, nel rispetto dei dettami del regolamento di voto. Il set di dati è definito nel contratto di servizio.
I dati personali sono trattati con modalità e strumenti consolidati costruiti appositamente per la gestione di processi e dati di votazioni.
ESATTEZZA, COMPLETEZZA, AGGIORNAMENTO
I dati personali sono puntualmente verificati e validati anche dal Titolare degli stessi in modo che sia garantita la loro esattezza, completezza ed aggiornamento nelle modalità previste da specifico contratto di servizi.
CONSERVAZIONE
I dati personali sono conservati per un periodo di tempo limitato al raggiungimento delle finalità dichiarate nel contratto.
SICUREZZA
i dati sono sempre raccolti e trattati successivamente alla verifica delle misure di sicurezza dichiarate ed adottate e previste nello specifico contratto che disciplina il servizio.
RISERVATEZZA
i dati sono trattati esclusivamente dai nostri specialisti, autorizzati dal Responsabile del trattamento.
gli specialisti coinvolti hanno tutti una pluriennale esperienza nella conduzione di votazioni elettroniche e del contesto normativo sulla privacy e GDPR su cui sono istruiti e periodicamente aggiornati.

ART. 6
Liceità del trattamento
Il trattamento avviene, da parte di ID Technology, in qualità di Responsabile esterno dei dati per l'esecuzione di attività relative alle votazioni periodiche del Titolare committente. I dati personal trattati saranno quindi solo ed esclusivamente relativi alla conduzione del servizio di votazione elettronica e nel rispetto del diritto dei votanti a votare.

ART. 7
Condizioni per il consenso
Trattandosi dell'esecuzione di un contratto e prestazione di servizio per l'esecuzione di Votazioni di un committente, Titolare dei dati, non è condizionato dal consenso esplicito degli appartenenti alle liste degli aventi diritto (elettorato attivo e passivo)
ART. 8

Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione

Non è previsto il recepimento di dati di minorenni aventi meno di 16 anni.

ART. 9

Trattamento di categorie particolari di dati personali

Non vengono trattate categorie particolari di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

Richiesta

Descrizione dell'adeguatezza all'Informazione e accesso ai dati personali (artt. dal 13 al 21)

Testo articolo 13 – http://www.privacy-regulation.eu/it/13.htm
Testo articolo 14 - http://www.privacy-regulation.eu/it/14.htm
Testo articolo 15 –http://www.privacy-regulation.eu/it/15.htm
Testo articolo 16 –http://www.privacy-regulation.eu/it/16.htm
Testo articolo 17 - http://www.privacy-regulation.eu/it/17.htm
Testo articolo 18 - http://www.privacy-regulation.eu/it/18.htm
Testo articolo 19 - http://www.privacy-regulation.eu/it/19.htm
Testo articolo 20 - http://www.privacy-regulation.eu/it/20.htm
Testo articolo 21 - http://www.privacy-regulation.eu/it/21.htm

ART. 13

Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

Il sistema di voto non raccoglie dati direttamente dagli interessati (elettori e candidati). I dati anagrafici degli elettori sono trasferiti dal Titolare ad ID Technology, al fine esclusivo di consentire il caricamento delle liste elettorali nel sistema di voto.

ART. 14 –

Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

Il Titolare conferisce i dati al fine di esclusivo della conduzione delle elezioni. A tal fine avrà già ricevuto le informazioni previste nel contratto di conferimento Responsabile esterno trattamento dati.

ART. 15

Diritto di accesso dell'interessato

ID Technology in qualità di Responsabile esterno del trattamento, consente l'accesso ai dati solo ed esclusivamente al Titolare degli stessi

ART. 16 –

Diritto di rettifica

Ogni elettore avrà facoltà di richiedere al cliente titolare dei dati la rettifica dei propri dati personali.
ID Technology provvederà ad eventuali rettifiche richieste documentate dal cliente o renderà disponibile una interfaccia di modifica sulle categorie di dati concordate (si rimanda contratto)

ART. 17 – Diritto alla cancellazione («diritto all'oblio»)
Tale diritto riferito ai dati personali non è esercitabile essendo relativo ai dati di una votazione a valenza legale, per cui è previsto un periodo di conservazione dei dati a cura del Titolare.

ART. 18 –
Diritto di limitazione di trattamento

Non esercitabile

ART. 19 –
Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento
E' un obbligo in capo al Titolare, ID Technology fornisce un supporto tecnico qualora fosse richiesto

ART. 20 –
Diritto alla portabilità dei dati
ID Technology rende disponibili i dati relativi alle votazioni in formato PDF non modificabile atto alla conservazione costitutiva. Rendiamo, inoltre, disponibili i dati anche, in formato XML (risultati di scrutinio, elenco votanti ...). Tale formato garantisce un'ampia portabilità su altri sistemi

ART. 21
Diritto di opposizione

Il diritto di opposizione può essere esercitato nei confronti del cliente che potrà avvalersi del nostro supporto per le esecuzioni delle attività

Richiesta
Descrizione dell'adeguatezza delle misure tecniche ed organizzative (artt.24,25,32)

Testo articolo 24 - http://www.privacy-regulation.eu/it/24.htm
Testo articolo 25 - http://www.privacy-regulation.eu/it/25.htm
Testo articolo 32 - http://www.privacy-regulation.eu/it/32.htm

Risposta
ART. 24
Responsabilità del titolare del trattamento

ART. 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

I sistemi messi a disposizione dal cloud prescelto di Aruba soddisfano pienamente i suggerimenti legati alla protezione dei dati, per quanto riguarda le tecniche di sicurezza adottate dall'infrastruttura utilizzata (cap. 2.4.1).

ART. 32 - Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
b) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
c) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

2.4 Funzionalità generali del sistema di voto

2.4.1 Processo di voto

La piattaforma **ELIGO** garantisce una completa rispondenza alle esigenze elettorali dell'Ente.

a. Il servizio di voto **ELIGO** offerto da ID Technology è stato verificato dall'ente "**Garante per la protezione dei dati**" riguardante la conformità del Servizio alla disciplina, di cui al D.lg. n.196/2003, relativa ai trattamenti dei dati personali e alla sicurezza ed anonimato del voto, che l'ha ritenuto conforme alla normativa italiana ed europea sia per quanto attiene il processo di trattamento dei dati sia per la segretezza delle preferenze espresse durante le votazioni.

b. Il sistema **ELIGO** prevede che ogni elettore avente diritto di voto possa accedere alla piattaforma utilizzando il proprio Codice iscritto e relativa password, normalmente utilizzati dagli iscritti INPGI per accedere ai servizi on-line dell'Ente. In questo senso il sistema di voto demanda totalmente ai sistemi di autenticazione INPGI il corretto riconoscimento delle credenziali indicate durante l'accesso alla cabina di voto.

Figura 1 - Pagina di accesso al servizio di voto

A valle dell'avvenuto riconoscimento delle credenziali indicate nella pagina di accesso, ELIGO provvede a verificare che l'iscritto abbia il diritto di votare, ed in caso positivo richiede all'elettore di indicare un proprio numero di cellulare ove recapitare un codice PIN per proseguire con l'accesso al sistema.
Il numero di cellulare subisce una serie di controlli automatici da parte del sistema ELIGO, accertando che non sia un numero "usa e getta" fornito da diversi siti web e che non sia già stato attribuito ad altri iscritti.
Verificate positivamente le precedenti condizioni, ELIGO genera automaticamente un codice PIN e lo invia tramite SMS al cellulare dell'iscritto indicato.
L'elettore deve riportare nella pagina di accesso al voto il codice PIN ricevuto entro 1 minuto dalla sua emissione, pena l'annullamento automatico della procedura di accesso (che riporta l'elettore allo stato inziale dell'accesso).

Figura 2 - Invio PIN via SMS

Si ricorda che ogni PIN viene generato automaticamente dalla piattaforma di voto, inviato al numero di cellulare indicato e quindi crittografato in modalità "one way" sulla base dati sottostante il servizio di voto. Neanche noi in qualità di fornitori del servizio siamo in grado di risalite al pin inviato leggendo il dato dalla base dati ove archiviato.

ELIGO prevede che a seguito della procedura di accesso al servizio degli elettori, venga automaticamente mostrata la prima scheda di voto in cui l'elettore è chiamato ad esprimere le proprie preferenze. La parte superiore della scheda di voto riporta sempre l'indicatore del totale delle schede di voto assegnate al votante, evidenziando la scheda di voto correntemente aperta. Il sistema prevede che ogni votante venga automaticamente disconnesso se oltrepassato un numero di minuti massimi di inattività (valore configurabile).

L'elettore provvede a votare per l'organo previsto selezionando i nominativi dei Candidati, spuntandoli dall'elenco nel numero massimo di preferenze stabilito.
Poiché il voto non comporta la digitazione libera di nominativi, l'elettore non può annullare la scheda; può invece esprimere scheda bianca se non indica alcuna preferenza nella scheda di voto.
Viene richiesta ad ogni votante la conferma delle preferenze indicate, espressa sul riepilogo delle preferenze selezionate (o sulla scelta di scheda bianca). Il voto nullo non è ammesso.

A conferma avvenuta, la piattaforma registra in modo scisso e separato che l'elettore ha votato e deposita il voto in modo crittografato ed immodificabile in un database dedicato. Viene nativamente impedito dalla piattaforma il doppio voto.

A completamento della registrazione del voto per il primo Organo, il sistema avverte l'elettore della corretta registrazione del voto e mostra la scheda di voto per l'organo successivo. Il processo prosegue allo stesso modo per tuti gli Organi per cui l'elettore deve provvedere a votare. Al termine dell'assegnazione del voto per l'ultimo Organo il sistema conferma all'elettore il completamento delle operazioni voto, impedendogli di poter votare nuovamente.

Per la piena segretezza, in ELIGO non viene registrato alcun legame tra voto espresso e votante e, per impedire qualunque anticipazione del risultato a urne aperte, il voto viene viene crittografato secondo le specifiche dell'algoritmo RSA a chiave asimmetrica (a doppia chiave).

c. Le comunicazioni tra votante e sistema di voto centrale vengono crittografate tramite connessione cifrata su protocollo https (certificato SSL) mediante certificato digitale a 256 bit.

d. Il sistema di voto **ELIGO** adotta elevati criteri di sicurezza, necessari per garantire il migliore funzionamento e la protezione da attacchi malevoli.
I dati relativi alle preferenze espresse (voti) sono mantenuti (in modalità crittografata) all'interno dell'apposito database impedendone la leggibilità ed alterazione, anche al fornitore del software di voto.
Per impedire eventuali furti della base dati, questa è automaticamente crittografata attraverso la modalità TDE (Transparent Data Encryption) che impedisce la possibilità di trasferire altrove i dati presenti nella base dati stessa.

e. All'atto della chiusura delle votazioni, la cabina elettorale viene definitamente chiusa dal personale ID Technology presente presso la sede INPGI, in presenza del notaio nominato dall'Ente, nel giorno e nell'ora previste dal regolamento elettorale.
Non sarà più consentito nessun accesso alla cabina di voto dopo la sua chiusura. Il sistema viene disconnesso da internet.
Il notaio accerta in questa fase il numero di voti registrati a valle della chiusura del voto.

f. Al momento del voto l'informazione voto / votante viene definitivamente persa e non potrà mai più essere ricostruita.

Ogni operazione di voto viene tracciata in una opportuna tabella del sistema **ELIGO**. Oltre alle azioni esercitate dai votanti (con esclusione delle scelte sulle preferenze espresse) vengono memorizzati anche gli indirizzi IP delle postazioni dalle quali vengono esercitati i voti.

Per la piena segretezza, in ELIGO non viene registrato alcun legame tra voto espresso e votante ed il voto memorizzato in un database dedicato.
Viene nativamente impedito dalla piattaforma il doppio voto.

g. Viene garantito un elevato livello di sicurezza sui dati mediante l'utilizzo di due base dati distinte, dove i dati sensibili vengono mantenuti crittografati.
La prima base dati contiene i dati relativi ai votanti.
La seconda base dati contiene i dati relativi ai voti sottomessi.

h. L'alimentazione dell'elettorato attivo e passivo avviene attraverso l'importazione di un file in formato Excel standard ricevuto e validato dall'Ente. Post caricamento vengono verificati dall'Ente i dati relativi ai dati caricati.

i. Unitamente al sistema di voto viene incluso il servizio di manutenzione ed assistenza per il periodo elettorale. Viene qui garantito il ripristino del corretto funzionamento del sistema di voto al verificarsi di malfunzionamenti o errori.

2.4.2 Definizione lista elettori

Il sistema di voto prevede che la lista degli aventi diritto di voto per ogni votazione venga prima preparata in un file excel e quindi caricata sul sistema di voto.

Figura 3 - Caricamento lista elettori

Il file excel deve contenere almeno le colonne identificativo, nome, cognome ed opzionalmente l'indirizzo di posta elettronica degli aventi diritto di voto.
Tale file deve essere caricato nella relativa votazione tramite un semplice upload da interfaccia web.

2.4.3 Accessibilità del servizio di voto

ELIGO è un sistema di voto elettronico esposto via web, accessibile da qualunque postazione internet dotata di un web browser e da qualsiasi device (smartphone, pc, tablet) senza necessità di installazione locale di altri software.

L'accesso al voto è regolato centralmente e quindi è possibile aprire e chiudere simultaneamente tutte le votazioni, senza riferimenti al tempo locale della postazione di voto.

Ogni elettore potrà accedere alla cabina di voto attraverso una apposita pagina di accesso dove verrà richiesto l'inserimento del codice iscritto INPGI (username) e relativa password. Il secondo fattore di autenticazione richiede l'indicazione del numero di cellulare dell'iscritto, dove verrà inviato un PIN per completare l'accesso.

2.4.4 Gestione della Cifratura a doppia chiave

Eligo provvede a crittografare i voti registrati nell'urna digitale secondo l'algoritmo RSA.
La crittografia eseguita sui voti è del tipo “Asimmetrica”, tramite la quale i voti sono registrati e crittografati secondo una chiave pubblica e possono essere de-crittografati esclusivamente tramite una opportuna chiave privata (si ricorda che un voto de crittografato non contiene comunque il legame voto/votante).

La chiave di de-crittazione dei voti viene consegnata in anticipo rispetto all’apertura del voto al notaio indentificato da INPGI che la dovrà sottomettere al sistema per le procedure di spoglio previste.

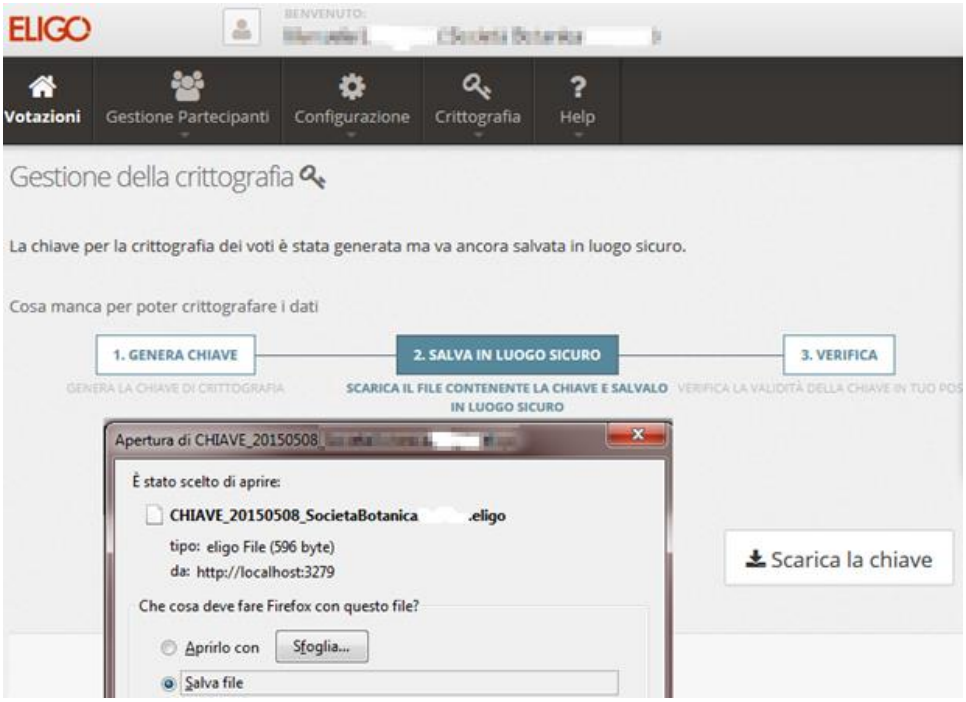

Figura 4 - Processo di consegna e verifica chiave privata

Il responsabile incaricato di mantenere la chiave privata (il notaio) conserverà la stessa (salvata in un opportuno file) fino alla chiusura delle votazioni, momento durante il quale tale chiave dovrà essere inviata al sistema di voto eligo per effettuare lo spoglio.

2.4.5 Scrutinio e Report finali

Ad urne aperte, **ELIGO** mette a disposizione ai profili qualificati il **dato di affluenza** (percentuale dei votanti rispetto agli aventi diritto, distinta per ogni Organo). A seguito della chiusura di ogni votazione, e richiesto lo **scrutinio dei voti,** il sistema di voto **produrrà per la commissione elettorale i** reports riportanti l'elenco dei voti ricevuti da ogni candidato per la determinazione degli eletti di ogni organo.

I reports per ogni Organo conterranno le seguenti informazioni:

- dati della votazione (Organo, date di apertura del voto)
- l'elenco ed il numero degli aventi diritto in anagrafe
- l'elenco nominale ed il numero dei votanti
- il numero di schede bianche
- l'elenco nominale dei candidati disposti in ordine decrescente di preferenze ricevute.