



DELLA LOMBARDIA

Prot. N. 557/2022

Assago (MI), 3 ottobre 2022

AVVISO PER ATTRIBUZIONE DI INCARICO

CAPITOLATO TECNICO PER LA SELEZIONE DEL FORNITORE DELLA PIATTAFORMA PER IL VOTO TELEMATICO

A. Approvvigionamento della piattaforma di voto telematico.

1. L'acquisizione della soluzione *software* o del servizio in *cloud* deve avvenire nel rispetto dei principi individuati dagli artt. 68 e 69 del Codice dell'amministrazione digitale, relativamente a criteri di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica. Verrà privilegiata l'acquisizione di una soluzione che consenta di sfruttare i vantaggi dell'economia di scala (*software-as-a-service* ovvero *software open source*), ferma restando in capo all'Ordine la facoltà di non rendere pubblico il codice sorgente in considerazione delle motivate esigenze di cui all'art. 69 comma 1, ultimo inciso.
2. Nel caso in cui la soluzione *software* acquisita sia dotata di licenza *open source*, è comunque facoltà dell'Ordine di pubblicare, modificare e procedere alla manutenzione della stessa secondo il disposto delle Linee guida su acquisizione e riuso di *software* per le pubbliche amministrazioni adottate con determinazione dell'Agenzia per l'Italia digitale n. 115/2019 del 9 maggio 2019.
3. Indipendentemente dal tipo di licenza adottata, il fornitore dovrà mettere a disposizione dell'Ordine il codice sorgente della soluzione *software* nella sua integralità ai fini di ispezione ed *auditing* di sicurezza, nonché consentire in ogni momento, attraverso tecniche di compilazione deterministica (c.d. "*deterministic compilation*" o "*reproducible build*") e firmando digitalmente i *file* eseguibili, che il *software* eseguito all'interno della piattaforma in produzione (*on premise* ovvero in *cloud*) corrisponda esattamente al codice sorgente.
4. In caso di acquisizione di soluzioni *software* in *cloud*, il fornitore dovrà essere in possesso di qualificazione ai sensi delle Circolari dell'Agenzia per l'Italia digitale n. 2 e n. 3 del 9 aprile 2018.

B. Documentazione

1. La soluzione acquisita deve essere provvista di documentazione a corredo, adeguatamente dettagliata e aggiornata, resa in formato documentale aperto e contenente almeno le seguenti parti:
 - a) una descrizione di carattere generale della soluzione in forma di sommario esecutivo redatta in linguaggio non tecnico;
 - b) una discussione tecnica della soluzione corredata di discussione delle scelte progettuali e implementative;

- c) una descrizione formale e *machine-readable* dell'architettura della piattaforma, preferibilmente resa in conformità a *framework* universalmente diffusi (TOGAF ovvero EIRA);
- d) un elenco delle certificazioni eventualmente in possesso della soluzione;
- e) una descrizione delle modalità di esportazione dei dati;
- f) una o più policy di sicurezza applicativa, di identity management, di gestione dei log;
- g) una attestazione sulla adeguata disponibilità di incident report, di statistiche e di strumenti di monitoraggio;
- h) una griglia di compatibilità con hardware, sistemi operativi, database, altri software applicativi, browser, dispositivi od altri asset digitali rilevanti per le operazioni di voto telematico.

2. Nell'ipotesi di soluzione *on premise*, la documentazione di cui al comma precedente deve essere integrata da:

- a) una descrizione dell'ambiente di produzione, di eventuali ambienti di test o di collaudo e dei corrispondenti requisiti;
- b) una stima del costo totale di possesso (c.d. TCO) corrispondente al livello di servizio richiesto, inclusi i costi di formazione del personale;
- c) motivate ragioni della deroga al principio Cloud First di cui al Piano triennale per l'informatica nella Pubblica Amministrazione 2020-2022.

3. Nell'ipotesi di soluzione in *cloud*, la documentazione di cui al comma precedente deve essere integrata dall'indicazione di tutti i requisiti aggiuntivi rispetto a quelli previsti dalla procedura di qualificazione di servizi per il *Cloud* della PA di cui al paragrafo A, numero 4, del presente capitolato, che il fornitore si impegna a porre in essere per garantire il livello di servizio richiesto.

4. Il fornitore deve inoltre produrre per quanto di rilevanza ai fini del presente Regolamento:

- 1. un organigramma della propria struttura organizzativa;
- 2. una descrizione delle *policy* di *data governance*;
- 3. una attestazione delle certificazioni possedute, tra le quali è da considerarsi obbligatoria la UNI EN ISO 9001:2015 e successivi aggiornamenti o altra certificazione equivalente in materia di gestione della qualità.

C. Codice sorgente

1. Il codice sorgente della soluzione acquisita deve presentare elevate caratteristiche di qualità, robustezza e scalabilità *by design*, delle quali dovrà essere specificata la misurabilità sulla base di metriche e indicatori concordati.

2. Dovrà essere possibile in qualsiasi momento da parte dell'Ordine o di terzi da questo delegati la verifica della correttezza formale del codice e la rispondenza ai requisiti di qualità attraverso l'applicazione di schemi di valutazione emanati da organismi internazionali di standardizzazione, tra i quali lo ISO/IEC 25010:2011, nonché di tecniche di analisi statica e dinamica.

D. Autenticazione e autorizzazione

1. Tutti gli accessi alla soluzione *software* individuata, ivi compresi quelli dotati di privilegi amministrativi, dovranno avvenire attraverso l'utilizzo combinato di codice fiscale e di password trasmessa dal Referente tecnico a mezzo posta elettronica certificata ovvero attraverso il Sistema

Pubblico di Identità Digitale o la Carta d'Identità Elettronica, ai sensi dell'art. 64 del Codice dell'amministrazione digitale.

2. In caso di autenticazione con SPID, è richiesto un livello di sicurezza pari almeno a due per gli accessi ordinari e pari a tre per gli accessi dotati di privilegi amministrativi. Nell'ipotesi in cui l'utente dotato di privilegi amministrativi non sia in possesso di SPID di livello tre è consentito l'uso di un livello di sicurezza pari a due purché integrato con l'uso di un dispositivo fisico di autenticazione erogato dal fornitore della piattaforma di voto.

E. Firma digitale con SPID

1. Si raccomanda che la piattaforma di voto supporti la sottoscrizione elettronica dei documenti ai sensi delle Regole Tecniche di cui all'art. 20 del Codice dell'amministrazione digitale.

F. Interoperabilità e cooperazione applicativa

1. La piattaforma di voto telematico deve garantire il rispetto dei principi di interoperabilità individuati con la Circolare n. 1 del 9 settembre 2020 dall'Agenzia per l'Italia digitale (c.d. modello di interoperabilità).

2. Ai fini di una gestione ottimale delle anagrafiche, la piattaforma di voto telematico deve essere dotata di integrazione *machine-to-machine* con il sistema informativo preposto alla gestione dell'Albo dell'Ordine, assicurando tempi di aggiornamento adeguati al buon andamento delle procedure di voto.

3. La piattaforma di voto telematico può essere integrata, laddove l'Ordine lo ritenga opportuno e laddove si ravvisino adeguate caratteristiche di rappresentatività, efficienza e sicurezza, con il punto unico di accesso telematico (c.d. "app IO") attivato presso la Presidenza del Consiglio dei ministri ai sensi dell'art. 64-*bis* del Codice dell'amministrazione digitale.

G. Sicurezza cibernetica

1. In considerazione dell'estrema sensibilità delle procedure di voto telematico sotto il profilo del governo degli Ordini, è necessario porre in essere tutte le misure di carattere organizzativo e tecnico necessarie per assicurare il corretto svolgimento delle operazioni nel rispetto delle garanzie procedurali, della normativa in materia di sicurezza cibernetica e di protezione dei dati personali, degli standard internazionali e nazionali (ivi incluso lo standard ISO/IEC 27001) e delle buone pratiche riconosciute dagli organismi comunitari (ENISA) e nazionali (ivi inclusi CISR, DIS, CERT-PA, CSIRT) competenti e dal Ministero della Salute nell'esercizio delle sue funzioni di autorità competente NIS ai sensi del decreto legislativo 18 maggio 2018, n. 65.

2. Limitatamente alle procedure di voto telematico, e fatta salva ogni disposizione di legge in materia, sono in capo all'Ordine gli stessi obblighi in materia di sicurezza e notifica degli incidenti che sono prescritti per gli operatori di servizi essenziali ai sensi della Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, e in conformità con le relative Linee Guida.

H. Protezione dei dati personali

1. Ricorrendo le fattispecie previste dall'art. 35 e dai Considerando 75, 84 e 89 del Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR), il trattamento dei dati personali necessario per le finalità connesse con le operazioni di voto elettronico e telematico è subordinato ad una valutazione dell'impatto (DPIA) del trattamento stesso sulla protezione dei dati personali.

2. L'informativa privacy resa ai sensi dell'art. 13 del predetto Regolamento deve essere redatta in conformità con i principi del *legal design*.

I. Tecnologie basate su registri distribuiti

1. Si intendono per tecnologie basate su registri distribuiti e per *smart contract* rispettivamente le tecnologie e i protocolli informatici e i programmi per elaboratore definiti ai commi 1 e 2 dell'art. 8-ter del d.l. 14 dicembre 2018, n. 135, convertito nella legge del 11 febbraio 2019, n. 12.

2. L'adozione di tecnologie basate su registri distribuiti e di *smart contract* dovrà tenere conto dell'individuazione da parte dell'Agenzia per l'Italia digitale degli standard tecnici che le stesse devono possedere affinché vengano prodotti gli effetti di identità certa e di validazione temporale elettronica di cui all'articolo 41 del Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014.

3. In nessun caso l'adozione di tecnologie basate su registri distribuiti e su *smart contract* può derogare ai requisiti generali per le operazioni di voto telematico ed elettronico.

L. Accessibilità

1. Tutte le interfacce utente della piattaforma di voto telematico ed elettronico devono conformarsi ai principi generali e alle prescrizioni tecniche della legge 9 gennaio 2004, n. 4 (*“Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici”*), nonché alle Linee Guida sull'Accessibilità degli strumenti informatici emanate dall'Agenzia per l'Italia digitale e in vigore dal 10 gennaio 2020.

M. Conservazione

1. Tutti i documenti informatici rilevanti per le operazioni di voto telematico ed elettronico, ivi inclusi il codice sorgente e i file eseguibili del *software*, i documenti di valutazione dei rischi, i log dei sistemi informatici, i verbali del seggio elettorale, gli esiti dello scrutinio, formano un pacchetto informativo di cui è fatto obbligo all'Ordine di procedere alla conservazione ai sensi degli art. 43 e 44 del Codice dell'amministrazione digitale e delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici adottate dall'Agenzia per l'Italia digitale.

2. La piattaforma di voto si integra con il servizio di conservazione dell'Ordine ovvero fornisce autonomamente un proprio servizio di conservazione purché conforme alle politiche e ai requisiti di carattere generale del servizio di conservazione dell'Ordine stesso. Le disposizioni del manuale di conservazione dell'Ordine, ove presente, si applicano sempre nella parte in cui esse non siano meno restrittive di quanto previsto nel Regolamento adottato dall'Ordine.

3. Quale ulteriore misura di tutela della trasparenza e dell'integrità informativa, la piattaforma di voto può, con modalità e cadenza opportunamente definite, registrare le impronte digitali dei pacchetti informativi (c.d. *“notarizzazione”*) di cui al comma 1 tramite tecnologie basate su registri distribuiti, con le limitazioni di cui al paragrafo I.