DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 9 settembre 2022

Disciplina della piattaforma per la raccolta delle firme degli elettori necessarie per i referendum previsti dagli articoli 75 e 138 della Costituzione. (22A06699)

(GU n.277 del 26-11-2022)

IL PRESIDENTE
DEL CONSIGLIO DEI MINISTRI

Vista la legge 23 agosto 1988, n. 400, recante «Disciplina dell'attivita' di governo e coordinamento della Presidenza del Consiglio dei ministri»;

Visti gli articoli 71, 75 e 138 della Costituzione;

Vista la legge 30 dicembre 2020, n. 178, recante «Bilancio di previsione dello Stato per l'anno finanziario 2021 e bilancio pluriennale per il triennio 2021-2023», e, in particolare, l'art. 1, commi 341, 342 e 343;

Vista la legge 25 maggio 1970, n. 352, recante «Norme sui referendum previsti dalla Costituzione e sulla iniziativa legislativa del popolo», e, in particolare, gli articoli 4, 7. 8, 27, 28 e 49;

Visto il decreto del Presidente della Repubblica 20 marzo 1967, n. 223, recante «Approvazione del testo unico delle leggi per la disciplina dell'elettorato attivo e per la tenuta e la revisione delle liste elettorali»;

Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante il «Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa»;

Visto il regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;

Visto il decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale»;

Visto il decreto del Presidente del Consiglio dei ministri 10 novembre 2014, n. 194, recante le modalita' di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (ANPR) e di definizione del piano per il graduale subentro dell'ANPR alle anagrafi della popolazione residente;

Visto il regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il «Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE»;

Visto il decreto del Presidente della Repubblica in data 12 febbraio 2021, con il quale il dott. Vittorio Colao e' stato nominato Ministro senza portafoglio;

Visto il decreto del Presidente del Consiglio dei ministri in data 13 febbraio 2021 con il quale al Ministro senza portafoglio dott. Vittorio Colao e' stato conferito l'incarico per l'innovazione tecnologica e la transizione digitale;

Visto il decreto del Presidente del Consiglio dei ministri in data 15 marzo 2021 con il quale al Ministro senza portafoglio dott. Vittorio Colao e' stata conferita la delega di funzioni;

Sentito il Garante per la protezione dei dati personali che si e' espresso con provvedimento n. 106 del 24 marzo 2022;
Acquisito il concerto del Ministro della giustizia;

Decreta:

Art. 1

Definizioni

1. Ai fini del presente decreto si intendono per:
a. «ANPR»: l'Anagrafe nazionale della popolazione residente di cui all'art. 62 del CAD;
b. «CAD»: il decreto legislativo 7 marzo 2005, n. 82, recante «Codice dell'amministrazione digitale»;
c. «piattaforma»: la piattaforma per la raccolta delle firme degli elettori necessarie per i referendum e le iniziative popolari, realizzata ai sensi dell'art. 1, comma 341 della legge 30 dicembre 2020, n. 178, recante «Bilancio di previsione dello Stato per l'anno finanziario 2021 e bilancio pluriennale per il triennio 2021-2023»;
d. «GDPR»: il regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016;
e. «gestore della piattaforma»: la persona giuridica a cui la Presidenza del Consiglio dei ministri affida la realizzazione, la gestione e la manutenzione della piattaforma;
f. «portale»: l'interfaccia web della piattaforma accessibile all'indirizzo www.firmereferendum.gov.it;
g. «regolamento eIDAS»: il regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio del 23 dicembre 2014.

Art. 2

Oggetto

1. Il presente decreto disciplina le modalita' di funzionamento della piattaforma, definendone le caratteristiche tecniche, l'architettura generale, i requisiti di sicurezza, le modalita' di funzionamento, i casi di malfunzionamento, le modalita' con cui il gestore della piattaforma attesta il malfunzionamento e comunica il ripristino delle funzionalita', le modalita' di accesso, le tipologie di dati oggetto di trattamento, le categorie di interessati e, in generale, le modalita' e le procedure per assicurare il rispetto del GDPR. Definisce, inoltre, le modalita' con cui i promotori della raccolta firme mettono a disposizione della Corte di cassazione le firme raccolte elettronicamente.

Art. 3

Infrastruttura tecnologica, requisiti di sicurezza, piano di test per la verifica del corretto funzionamento e malfunzionamenti

1. Il gestore della piattaforma sviluppa l'infrastruttura tecnologica, applicando i criteri di accessibilita' di cui alla legge 9 gennaio 2004, n. 4, nel rispetto dei principi di usabilita', completezza di informazione, chiarezza di linguaggio, affidabilita', semplicita' di' consultazione, qualita', omogeneita' e interoperabilita'.
2. Prima della sua messa in funzione, il gestore della piattaforma verifica e attesta il corretto funzionamento della stessa piattaforma tramite lo svolgimento di test sperimentali. Il piano dei test copre la totalita' dei casi d'uso e delle funzionalita' assegnate alla piattaforma dall'art. 1, commi 341 e 343, della legge 30 dicembre 2020, n. 178.
3. Le caratteristiche tecniche, le regole tecniche e i requisiti di sicurezza della piattaforma sono descritti nel manuale operativo redatto dal gestore della piattaforma, allegato al presente decreto, pubblicato sul sito web dello stesso gestore e sul portale. Nel manuale sono individuate le metriche di successo e fallimento delle operazioni eseguite, unitamente a metriche prestazionali e di qualita', nonche' di assistenza agli utenti. Tali metriche sono utilizzate per monitorare l'operativita' della piattaforma.

4. Costituiscono casi di malfunzionamento della piattaforma tutti gli impedimenti tecnici, rilevati anche automaticamente dal sistema con le modalita' di cui al comma 3, che rendono impossibile la raccolta delle firme degli elettori.

5. Il malfunzionamento della piattaforma viene segnalato sul portale. Con le stesse modalita' il gestore della piattaforma comunica il ripristino della funzionalita' della stessa piattaforma.

6. Il gestore della piattaforma cura la manutenzione della stessa e provvede al suo aggiornamento tecnologico, d'intesa con il Dipartimento per la trasformazione digitale e sentito il Garante per la protezione dei dati personali per gli aspetti di competenza.

Art. 4

Architettura e funzionamento della piattaforma

1. La piattaforma, accessibile tramite il portale, e' organizzata in un' «area pubblica» ed in un' «area privata» .

2. L'area pubblica consente la consultazione delle proposte referendarie e dei relativi quesiti nonche' delle proposte di legge popolare, in corso e scadute, con l'indicazione del numero di firme raccolte fino al momento della visualizzazione. Consente, altresi', la consultazione di tutte le informazioni necessarie per partecipare alla raccolta delle firme mediante la stessa piattaforma.

3. L'area privata, a cui e' possibile accedere mediante un'identita' digitale basata su credenziali di livello almeno significativo nell'ambito di un regime di identificazione elettronica oggetto di notifica, conclusa con esito positivo, ai sensi dell'art. 9 del regolamento (UE), n. 910/214, consente l'utilizzo delle funzionalita' della piattaforma diversificate in relazione atre distinte tipologie di utenti:

a. «utenza Corte di cassazione»: dedicata al personale della Corte di cassazione abilitato dal gestore mediante una specifica funzionalita' della piattaforma descritta nel manuale operativo di cui all'art. 3, comma 3.

L'abilitazione e' riconosciuta sulla base dei seguenti profili differenziati di accesso che tengono conto delle specifiche mansioni svolte dal suddetto personale:

1. profilo magistrato: dedicato alla consultazione, estrazione e controllo delle sottoscrizioni raccolte per le iniziative referendarie e depositate presso la Corte di cassazione nonche', piu' in generale, alle funzioni di cui agli articoli 12 e 32 della legge 25 maggio 1970, n. 352;

2. profilo personale tecnico-amniinistrativo: dedicato all'inserimento in piattaforma dei nominativi dei promotori della raccolta e all'abilitazione di almeno due promotori della raccolta ad operare sulla piattaforma;

3. profilo amministratore delle utenze: dedicato all'abilitazione e alla disabilitazione di ulteriore personale della Corte di cassazione sulla base di specifiche esigenze organizzative;

4. profilo personale delegato: dedicato al personale delegato di cui all'art. 2, del decreto-legge 9 marzo 1995, n. 67, convertito, con modificazioni, dalla legge 5 maggio 1995, n. 159;

b. «utenza Soggetti promotori»: dedicata ai soggetti promotori della proposta referendaria o di legge popolare abilitati:

1. al caricamento in piattaforma, successivamente alla pubblicazione nella Gazzetta Ufficiale dell'annuncio di cui all'art. 7, secondo comma, della legge 25 maggio 1970, n. 352, della proposta;

2. alla consultazione, estrazione e monitoraggio delle sottoscrizioni raccolte per l'iniziativa;

3. all'abilitazione di ulteriori soggetti promotori i cui nominativi sono inseriti in piattaforma ai sensi della lettera a), numero 2.

L'accesso ai dati personali dei sottoscrittori resta nella disponibilita' esclusiva dei promotori fino alla data del deposito delle medesime sottoscrizioni presso la cancelleria della Corte di cassazione;

c. «utenza Cittadino»: dedicata agli aventi diritto che intendono sottoscrivere una proposta referendaria o di legge popolare.

4. Il personale abilitato della cancelleria della Corte di cassazione, entro due giorni lavorativi dalla pubblicazione nella Gazzetta Ufficiale dell'annuncio di cui all'art. 7, secondo comma, della legge 25 maggio 1970, n. 352, inserisce in piattaforma il nome, il cognome, il luogo, la data di nascita, il codice fiscale e il comune di iscrizione nelle liste elettorali dei promotori della raccolta e abilita almeno due dei soggetti promotori in conformita' a quanto previsto al comma 3, lettera a), utilizzando una specifica funzionalita' descritta nel manuale operativo di cui all'art. 3, comma 3.

5. Il promotore abilitato, effettuato l'accesso alla piattaforma, abilita gli altri promotori dell'iniziativa, i cui nominativi sono inseriti in piattaforma ai sensi del comma 3, lettera a), numero 2, se non gia' abilitati dal personale tecnico-amministrativo della Corte di cassazione. Procede, inoltre, a caricare in piattaforma la proposta recante, a seconda delle finalita' della raccolta delle firme, le specifiche indicazioni prescritte, rispettivamente, dagli articoli 4, 27 e 49 della legge n. 352 del 1970, oltre agli ulteriori dati utili alla presentazione dell'iniziativa. Le attivita' di cui al presente comma sono eseguite mediante specifiche funzionalita' descritte nel manuale operativo di cui all'art. 3, comma 3.

6. La piattaforma, al termine del caricamento di cui al comma 5, tramite una specifica funzionalita' descritta nel manuale operativo di cui all'art. 3, comma 3, acquisisce la proposta e, rendendola immodificabile nel rispetto delle previsioni del CAD e delle linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici, le attribuisce data certa mediante l'apposizione di uno strumento di validazione temporale elettronica qualificata di cui all'art. 42 del regolamento eIDAS.

7. Contestualmente all'acquisizione di cui al comma 6, la piattaforma, mediante una specifica funzionalita' descritta nel manuale operativo di cui all'art. 3, comma 3, rende disponibile ai promotori un'attestazione di pubblicazione dell'iniziativa referendaria o di legge popolare munita di sigillo elettronico qualificato ai sensi del regolamento eIDAS. Rende altresi' disponibile la stessa iniziativa alla raccolta delle sottoscrizioni, per il periodo di tempo necessario a seconda delle finalita' della raccolta nel rispetto di quanto previsto dagli articoli 4, 28 e 49 della legge n. 352 del 1970, delle indicazioni fornite dai soggetti promotori all'atto del caricamento di cui al comma 5 e, comunque, non oltre la messa a disposizione della cancelleria della Corte di cassazione, da parte dei soggetti promotori, con le modalita' di cui all'art. 7, delle firme raccolte elettronicamente.

8. I promotori possono terminare la raccolta delle sottoscrizioni in qualsiasi momento utilizzando una specifica funzionalita' della piattaforma descritta nel manuale operativo di cui all'art. 3, comma 3.

9. La piattaforma, a partire dalla data in cui e' assicurata l'interoperabilita' con la PDND ovvero con l'Anagrafe nazionale della popolazione residente (ANPR), permette ai soggetti legittimati dalla legge, tramite una specifica funzionalita' descritta nel manuale operativo di cui all'art. 3, comma 3, la verifica della correttezza dei dati dei cittadini fruitori della stessa piattaforma nonche' della loro iscrizione nelle liste elettorali.

10. La piattaforma, fino a quando il dato relativo all'iscrizione nelle liste elettorali non e' disponibile in ANPR, consente ai soggetti promotori, mediante apposita funzionalita' descritta nel manuale operativo di cui all'art. 3, comma 3, di inviare al comune competente, con posta elettronica certificata o altro servizio elettronico di recapito certificato qualificato, la richiesta di verifica dell'iscrizione dei sottoscrittori nelle liste elettorali con rilascio del relativo certificato.

Art. 5

Modalita' di raccolta delle sottoscrizioni

1. L'avente diritto, dopo aver effettuato l'accesso alla piattaforma con le modalita' di cui all'art. 4, comma 3, sceglie la

proposta referendaria o di legge popolare che intende sottoscrivere recante, a seconda delle finalita' della raccolta firme, le specifiche indicazioni prescritte, rispettivamente, dagli articoli 4, 27 e 49 della legge 25 maggio 1970, n. 352.

2. La piattaforma, mediante una specifica funzionalita' descritta nel manuale operativo di cui all'art. 3, comma 3 e fatto salvo quanto previsto dall'art. 4, comma 10, acquisisce il nome, il cognome, il luogo e la data di nascita del sottoscrittore, il comune nelle cui liste elettorali e' iscritto ovvero, per i cittadini italiani residenti all'estero, la loro iscrizione nelle liste elettorali dell'Anagrafe degli italiani residenti all'estero, nonche', ove disponibile, l'attributo elettore presente in ANPR.

3. La piattaforma acquisisce, altresi', l'identificativo univoco della sessione di autenticazione fornito dal gestore di identita' digitale. Nel caso in cui tale identificativo non e' disponibile, lo stesso e' generato e associato alla sessione direttamente dalla piattaforma.

4. Le informazioni di cui ai commi 2 e 3 sono esposte al sottoscrittore, in relazione all'iniziativa prescelta, al momento della raccolta della firma espressa, con le modalita' descritte nel manuale operativo di cui all'art. 3, comma 3, e confermate dallo stesso mediante la pressione di un tasto dedicato alla sottoscrizione.

5. Le informazioni e le evidenze informatiche delle attivita' di cui ai commi 1, 2, 3 e 4 sono registrate e rese immodificabili nel rispetto delle disposizioni del GDPR e del CAD.

6. Il gestore della piattaforma garantisce la riconducibilita' della sottoscrizione all'avente diritto mediante certificazione di processo delle attivita' di cui ai commi 1, 2, 3 e 4 e apposizione al relativo documento del proprio sigillo elettronico qualificato, ai sensi del regolamento eIDAS. Le caratteristiche della certificazione di processo sono descritte nel manuale operativo di cui all'art. 3, comma 3.

Art. 6

Conservazione delle sottoscrizioni e diritto di accesso

1. Il gestore della piattaforma conserva le informazioni e le evidenze informatiche di cui all'art. 5, commi 1, 2, 3 e 4, per il medesimo periodo di tempo necessario alla verifica della validita' delle sottoscrizioni previsto per la conservazione delle firme raccolte con modalita' analogica, tramite memorizzazione nel rispetto delle disposizioni del GDPR e del CAD.

2. Gli utenti di cui all'art. 4, comma 3, lettera a), a partire dalla data del deposito delle sottoscrizioni presso la cancelleria della Corte di cassazione, possono accedere, mediante una specifica funzionalita' descritta nel manuale operativo di cui all'art. 3, comma 3, alle informazioni e alle evidenze informatiche conservate.

3. Gli utenti di cui all'art. 4, comma 3, lettera b), durante il periodo di conservazione, possono accedere, mediante una specifica funzionalita' descritta nel manuale operativo di cui all'art. 3, comma 3, esclusivamente alle informazioni e alle evidenze informatiche conservate, relative alle proprie proposte referendarie e di iniziativa popolare.

4. Gli utenti di cui all'art. 4, comma 3, lettera c), durante il periodo di conservazione, mediante una specifica funzionalita' descritta nel manuale operativo di cui all'art. 3, comma 3, possono accedere esclusivamente alle informazioni e alle evidenze informatiche relative alle proprie sottoscrizioni.

Art. 7

Messa a disposizione delle firme raccolte elettronicamente

1. I soggetti promotori, al termine del periodo di raccolta delle sottoscrizioni e, comunque, nella stessa data in cui effettuano il deposito di eventuali firme autografe raccolte per la medesima proposta referendaria, mettono a disposizione della cancelleria della Corte di cassazione, con una specifica funzionalita' descritta nel

manuale operativo di cui all'art. 3, comma 3, le firme raccolte elettronicamente comprensive delle informazioni e delle evidenze informatiche di cui all'art. 5, commi 1, 2, 3 e 4.

2. La piattaforma, contestualmente alla messa a disposizione delle firme e delle evidenze ai sensi del comma 1, rende disponibile ai promotori, tramite una specifica funzionalita' descritta nel manuale operativo di cui all'art. 3, comma 3, un'attestazione di messa a disposizione munita di sigillo elettronico qualificato e riferimento temporale qualificato, ai sensi del regolamento eIDAS.

3. I soggetti abilitati di cui all'art. 4, comma 3, lettera a), numero 1, successivamente alla messa a disposizione delle firme e delle evidenze di cui al comma 1, mediante una specifica funzionalita' descritta nel manuale operativo di cui all'art. 3, comma 3, eventualmente coadiuvati dal personale delegato di cui all'art. 4, comma 3, lettera a), numero 4, o dal personale tecnico-amministrativo di cui all'art. 4, comma 3, lettera a), numeri 2 e 3, in possesso delle necessarie competenze tecniche, verificano la validita' delle firme raccolte elettronicamente e comprensive delle informazioni e delle evidenze informatiche di cui all'art. 5, commi 1, 2, 3 e 4. La valutazione della tempestivita' della raccolta delle sottoscrizioni elettroniche nel rispetto di quanto previsto dagli articoli 4, 28 e 49 della legge n. 352 del 1970, e' effettuata mediante una specifica funzionalita' della piattaforma, descritta nel manuale operativo di cui all'art. 3, comma 3, che consente la verifica automatica della data in cui le stesse sottoscrizioni sono state raccolte.

4. Relativamente alle proposte di legge popolare, le firme raccolte elettronicamente, comprensive delle informazioni e delle evidenze informatiche di cui all'art. 5, commi 1, 2, 3 e 4, possono essere presentate al Presidente di una delle due camere, ai sensi dell'art. 49, della legge n. 352 del 1970, come duplicato informatico ai sensi dell'art. 1, comma 1, lettera i-quinquies), del CAD, ovvero come copia analogica di documento informatico dotata del contrassegno a stampa di cui all'art. 23, comma 2-bis, del medesimo codice. Il duplicato informatico e la copia analogica possono essere estratti mediante una specifica funzionalita' descritta nel manuale operativo di cui all'art. 3, comma 3.

6. I soggetti abilitati di cui all'art. 4, comma 3, lettera a), numero 1, successivamente alla messa a disposizione delle firme e delle evidenze di cui al comma 1, mediante una specifica funzionalita' descritta nel manuale operativo di cui all'art. 3, comma 3, possono estrarre i dati dei sottoscrittori digitali in un formato idoneo a garantire l'interoperabilita' con gli applicativi utilizzati dall'Ufficio centrale per il referendum presso la Corte di cassazione al fine di individuare eventuali duplicazioni di sottoscrizioni raccolte sia elettronicamente sia analogicamente. Per tale attivita' possono essere eventualmente coadiuvati dal personale delegato di cui all'art. 4, comma 3, lettera a), numero 4, o dal personale tecnico-amministrativo di cui all'art. 4, comma 3, lettera a), numeri 2 e 3, lettere b) e c), in possesso delle necessarie competenze tecniche.

Art. 8

Tipologie di dati oggetto di trattamento, categorie di interessati e procedure per assicurare il rispetto dell'art. 5 del regolamento UE 2016/679

1. Nell'ambito di operativita' della piattaforma, i dati personali oggetto del trattamento sono:

a. il nome, il cognome, il luogo, la data di nascita, il codice fiscale del personale dell'Ufficio centrale per il referendum presso la Corte di cassazione abilitato ai sensi dell'art. 4, comma 3, lettera a);

b. il nome, il cognome, il luogo di nascita, la data di nascita, il codice fiscale, il comune di iscrizione nelle liste elettorali ovvero l'iscrizione nelle liste elettorali dell'Anagrafe degli italiani residenti all'estero dei promotori della raccolta;

c. il nome, il cognome, il luogo, la data di nascita, il codice

fiscale, il comune di iscrizione nelle liste elettorali ovvero l'iscrizione nelle liste elettorali dell'Anagrafe degli italiani residenti all'estero dei soggetti sottoscrittori la proposta di referendum o di legge popolare e, ove disponibile l'attributo elettore presente in ANPR;

d. l'identificativo univoco della sessione di autenticazione fornito dal gestore dell'identita' digitale ovvero generato direttamente dalla piattaforma;

e. l'evidenza della sottoscrizione della proposta referendaria o di legge popolare.

2. I dati di cui al precedente comma 1, sono trattati dai soggetti di cui all'art. 4, comma 3, lettera a) e b), esclusivamente per lo svolgimento delle attivita' di rispettiva competenza nonche' dal gestore per garantire il corretto funzionamento del sistema.

3. I dati personali e tutti i dati afferenti l'utilizzo e la gestione del sistema sono conservati dal gestore con modalita' atte a garantirne la protezione mediante misure tecniche e organizzative idonee ad evitare trattamenti non autorizzati o illeciti, la perdita e la distruzione.

Art. 9

Disposizioni in materia di trattamento dei dati personali

1. I dati personali di cui all'art. 8 sono trattati esclusivamente per le finalita' inerenti la raccolta delle firme degli elettori necessarie per i referendum previsti dagli articoli 75 e 138 della Costituzione nonche' per i progetti di legge previsti dall'art. 71, secondo comma, della Costituzione.

2. Il gestore della piattaforma e' responsabile del trattamento dei dati raccolti attraverso la piattaforma e, in generale, di ogni altro dato inerente alla gestione di ogni attivita' strumentale all'utilizzo della stessa piattaforma.

3. I soggetti di cui all'art. 4, comma 3, lettera a) e b), trattano i dati di cui all'art. 8, comma 1, lettera a), b), c), d) ed e), quali titolari autonomi del trattamento ai sensi della legge n. 352 del 1970 e del presente decreto.

4. Al fine di assicurare ai soggetti di cui all'art. 4, comma 3, lettere a), b) c), l'accesso previsto dall'art. 6, il gestore della piattaforma conserva le firme raccolte elettronicamente, comprensive delle informazioni e delle evidenze informatiche di cui all'art. 5, commi 1, 2, 3 e 4, per il tempo previsto dallo stesso art. 6.

5. Il gestore implementa misure di sicurezza appropriate e specifiche per tutelare i diritti fondamentali e gli interessi delle persone fisiche.

6. I soggetti di cui all'art. 4, comma 3, lettera a) e b), effettuano, prima dell'inizio dell'attivita' di trattamento, la valutazione d'impatto ai sensi dell'art. 35, paragrafo 10, del GDPR e consultano il Garante per la protezione dei dati personali nei casi di cui all'art. 36 del GDPR. Nella valutazione d'impatto sono indicate, tra l'altro, le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nonche' le eventuali misure poste a tutela dei diritti e delle liberta' degli interessati.

7. Il gestore garantisce, mediante una specifica funzionalita' descritta nel manuale operativo di cui all'art. 3, comma 3, la conoscenza da parte dei titolari del trattamento, in maniera tempestiva, delle violazioni di sicurezza o di qualsiasi minaccia che comporti un rischio per la sicurezza e per i diritti e le liberta' degli interessati al trattamento.

Art. 10

Disposizioni finali

1. All'attuazione delle disposizioni di cui al presente decreto si provvede nei limiti delle risorse finanziarie, umane e strumentali disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.

2. Il presente decreto e' inviato ai competenti organi di controllo

e pubblicato nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 9 settembre 2022

p. Il Presidente
del Consiglio dei ministri
il Ministro per l'innovazione tecnologica
e la transizione digitale
Colao

Il Ministro della giustizia
Cartabia

Registrato alla Corte dei conti il 31 ottobre 2022
Ufficio di controllo sugli atti della Presidenza del Consiglio, del Ministero della giustizia e del Ministero degli affari esteri, reg. n. 2712

Allegato

SOGEI

PIATTAFORMA REFERENDUM
MANUALE OPERATIVO

INDICE

delle sottoscrizioni alla Corte di cassazione (art. 7, co. 2 del decreto)

6.5. Descrizione delle funzionalita' di estrazione del duplicato informatico e della copia analogica per le proposte di legge di iniziativa popolare (art. 7, co. 5 del decreto)

7. Accesso alle sottoscrizioni

7.1. Descrizione della funzionalita' per la verifica delle firme da parte della Corte di cassazione (art. 7, co. 3 del decreto)

7.1.1. Descrizione della funzionalita' di accesso alle sottoscrizioni e relative evidenze informatiche da parte dell'utenza «cassazione» (art. 6, co. 2 del decreto)

7.2. Descrizione della funzionalita' di estrazione dati da parte degli utenti della Corte di cassazione per controllo duplicazione sottoscrizioni (art. 7, co. 7 del decreto)

8. Descrizione delle caratteristiche tecniche, regole tecniche e requisiti di sicurezza dell piattaforma (art. 3, co. 3, del decreto)

8.1. Descrizione delle metriche di successo e fallimento delle operazioni eseguite, unitamente a metriche prestazionali e di qualita', nonche' di assistenza agli utenti per monitorare l'operativita' della piattaforma (art. 3, co. 3, del decreto)

8.2. Modalita' comunicazione data breach da parte del gestore (art. 9, co. 7 del decreto)

1. Obiettivo

Il presente manuale operativo e' finalizzato alla definizione delle procedure e alla descrizione delle funzionalita' che determinano la gestione della Piattaforma Referendum e iniziative popolari (di seguito «piattaforma») in attuazione della legge 30 dicembre 2020, n. 178, art. 1, ai commi 341-344 (legge di bilancio 2021) e del decreto XXX (di seguito «decreto»).

2. Organizzazione della piattaforma

La piattaforma e' organizzata in un'«area pubblica» ed in un'«area privata».

L'area pubblica consente la consultazione delle proposte referendarie e dei relativi quesiti nonche' delle proposte di legge popolare in corso e scadute, con l'indicazione di tutte le informazioni necessarie alla sottoscrizione, il numero di firme raccolte fino al momento della visualizzazione ed il numero necessario di firme ancora da raccogliere per il raggiungimento del quorum.

L'area privata consente, secondo le diverse tipologie di utenze previste, di gestire la proposta referendaria, monitorandone l'andamento e, nel caso, sottoscrivendo la proposta stessa.

3. Gestione delle utenze previste

Le diverse tipologie di utenti accedono all'area privata esclusivamente attraverso i sistemi SPID/CIE/CNS, a fronte dei quali viene generato un Access Token crittografato che permette la comunicazione tra la parte SPA (Single Page Application) ed i servizi REST della piattaforma; l'Access Token ha un time-to-live e viene invalidato al logout esplicito da parte dell'utente.

3.1. Descrizione della funzionalita' di abilitazione del profilo «utenza Corte di cassazione» (art. 4, lett. a) del decreto)

Il gestore della piattaforma, tramite la funzione adibita alla gestione degli utenti, inserisce i dati anagrafici (codice fiscale, nome, cognome, luogo e data di nascita) di uno o piu' utenti della Corte di cassazione da abilitare come profilo tecnico amministratore delle utenze (profilo «personale tecnico-amministrativo»). La piattaforma verifica la sola correttezza dei dati acquisiti attraverso l' interoperabilita' con il sistema ANPR, senza ulteriori verifiche.

Gli utenti della Corte di cassazione cosi' abilitati, tramite la funzione adibita alla gestione degli utenti, inseriscono i dati anagrafici (codice fiscale, nome, cognome, luogo e data di nascita) degli ulteriori utenti della Corte di cassazione da abilitare, distinguendoli nei diversi profili necessari:

A. profilo magistrato: dedicato alla consultazione, estrazione e controllo delle sottoscrizioni raccolte per le iniziative referendarie e depositate presso la Corte di cassazione nonche', piu' in generale, alle funzioni di cui agli articoli 12 e 32 della legge 25 maggio 1970, n. 352;

B. profilo personale tecnico-amministrativo: dedicato all' inserimento in piattaforma dei nominativi dei promotori della raccolta e all'abilitazione di almeno due promotori della raccolta ad operare sulla piattaforma;

C. profilo amministratore delle utenze: dedicato all'abilitazione e alla disabilitazione di ulteriori soggetti facenti parte dell'Ufficio centrale per il referendum presso la Corte di cassazione sulla base di specifiche esigenze organizzative;

D. profilo personale delegato: dedicato al personale delegato di cui all'art. 2, del decreto-legge 9 marzo 1995, n. 67, convertito, con modificazioni, dalla legge 5 maggio 1995, n. 159;

3.2. Descrizione della funzionalita' di abilitazione dei promotori da parte del personale della cancelleria della Corte di cassazione (art. 4, co. 4 del decreto)

L'utente della Corte di cassazione, profilo tecnico amministrativo, attraverso la funzione di gestione degli utenti, associa l'elenco degli utenti promotori all'identificativo univoco della proposta pubblicato in Gazzetta ufficiale attraverso l'inserimento dei dati anagrafici di ciascun utente promotore (codice fiscale, nome, cognome, luogo e data di nascita). La piattaforma verifica la sola correttezza dei dati attraverso l'interoperabilita' con il sistema ANPR, senza ulteriori verifiche.

L'utente della Corte di cassazione, profilo tecnico amministrativo, attraverso la funzione di gestione degli utenti, visualizza i dati anagrafici (nome, cognome, luogo e data di nascita) degli utenti promotori precedentemente censiti e ne abilita almeno due alla gestione della proposta attraverso la spunta di uno specifico flag di abilitazione.

L'utente promotore abilitato, tramite la funzione adibita alla gestione degli utenti, visualizza le proposte a lui associate e, nel caso, abilita ulteriori promotori alla gestione del quesito referendario o iniziativa popolare attraverso la spunta di uno specifico flag di abilitazione.

4. Gestione del quesito referendario o iniziativa popolare

4.1. Descrizione della funzionalita' relativa alle attivita' dei promotori in piattaforma (art. 4, co. 5 del decreto)

L'utente promotore abilitato alla gestione della proposta referendaria o iniziativa popolare, attraverso gli strumenti di gestione della piattaforma, acquisisce i dati specifici della proposta scegliendo la tipologia di iniziativa da registrare:

Referendum abrogativo (art. 75 della Costituzione);

Referendum costituzionale (art. 138 della Costituzione);

Legge di iniziativa popolare (art. 71 della Costituzione).

La piattaforma guida l'utente promotore nell'inserimento dei dati relativi alla proposta da sottoscrivere specificandone i dati a seconda della tipologia di iniziativa:

Tipo di iniziativa prevista dall'art. 138 della Costituzione

- Categoria
- Comitato
- Titolo
- Logo (eventuale)
- Descrizione breve
- Descrizione lunga
- Titolo legge costituzionale
- Data approvazione alla camera dei deputati
- Data approvazione al senato
- Data pubblicazione nella Gazzetta Ufficiale della legge
- Numero nella Gazzetta Ufficiale
- Quesito relativo alla richiesta

Tipo di iniziativa prevista dall'art. 75 della Costituzione

- Categoria
- Comitato
- Titolo
- Logo
- Descrizione breve
- Descrizione lunga
- Leggi di riferimento
- Quesito relativo alla richiesta

Tipo di iniziativa prevista dall'art. 71 della Costituzione

Categoria
Comitato
Titolo
Logo
Descrizione breve
Descrizione lunga
Titolo legge
Testo integrale

4.2. Descrizione della funzionalita' per l'acquisizione della proposta da parte della piattaforma (art. 4, co. 6 del decreto)

L'utente promotore visiona l'anteprima della richiesta di caricamento in piattaforma della proposta e conferma la correttezza dei dati inseriti. Con la selezione di un apposito tasto, l'utente promotore carica in piattaforma la proposta e avvia immediatamente la raccolta delle firme.

Ogni iniziativa caricata e' resa immodificabile tramite apposizione di Sigillo elettronico qualificato, in formato PAdES, del soggetto a cui la legge assegna la realizzazione ed evoluzione della Piattaforma ed e' munita di riferimento temporale tramite apposizione marca temporale qualificata di cui all'art. 42 del regolamento eIDAS, utilizzando un servizio remoto messo a disposizione da una CA qualificata.

A partire da questo documento viene elaborato un hash (SHA-256) che sara' apposto sull'attestato di sottoscrizione del cittadino.

Al promotore e' inibita qualsiasi funzione di modifica della proposta.

4.3. Descrizione della funzionalita' di messa a disposizione dell'attestazione di pubblicazione (art. 4, co. 7 del decreto)

L'utente promotore, dopo il caricamento della proposta in piattaforma, puo' utilizzare gli strumenti di gestione che permettono di:

1. scaricare l'attestato di attivazione della proposta referendaria in formato pdf munito di sigillo elettronico qualificato e marca temporale che attesta l'attivazione del quesito referendario/iniziativa popolare;
2. aggiungere un'immagine relativa all'iniziativa o un riferimento ad un sito internet esterno a scelta del promotore.

4.4. Modalita' di accesso dei promotori ai dati conservati (art. 6, co. 3 del decreto)

In qualunque momento il promotore, tramite gli strumenti di gestione, puo' accedere alle sottoscrizioni effettuate dai cittadini, verificarne l'andamento tramite accesso ai dati, estrarre settimanalmente, ovvero alla chiusura della raccolta, elenchi contenenti i dati relativi alle sottoscrizioni, suddivisi per comune di iscrizione nelle liste elettorali di appartenenza, sia in formato pdf munito di sigillo elettronico qualificato che in formato csv e contenente i seguenti dati:

Titolo del quesito referendario/iniziativa popolare
Codice fiscale
Nome, cognome, data di nascita, luogo di nascita
Timestamp della sottoscrizione
Comune di iscrizione nelle liste elettorali dichiarato (o confermato a seguito di chiusura della raccolta delle sottoscrizioni - si veda il successivo paragrafo 6.3)

5. Sottoscrizione del quesito referendario o iniziativa popolare

5.1. Descrizione della funzionalita' di acquisizione dei dati per la sottoscrizione della proposta (art. 5, co. 2 del decreto)

Il cittadino che intende sottoscrivere un'iniziativa referendaria accede all'area privata attraverso un'identita' digitale. La Piattaforma acquisisce 1' identificativo univoco della sessione (ID sessione) di autenticazione fornito dal gestore di identita' digitale. Nel caso in cui l'identificativo non sia disponibile la Piattaforma ne genera uno che associa alla specifica sessione.

Il cittadino visualizza il dettaglio dei dati significativi della proposta scelta.

5.1.1. Descrizione della funzionalita' di verifica della correttezza dei dati dei cittadini fruitori della stessa piattaforma tramite interoperabilita' con ANPR (anche via PDND) nonche' della loro iscrizione nelle liste elettorali (art. 4, co. 9 del decreto)

La piattaforma, attraverso il codice fiscale fornito dal provider dell'identita' digitale, accede al sistema ANPR e mostra al cittadino i propri dati anagrafici (nome, cognome, luogo e data di nascita).

La Piattaforma consente al cittadino di completare la scheda inserendo il comune nelle cui liste elettorali e' iscritto.

Con l'integrazione in ANPR delle liste elettorali, anche questa operazione sara' svolta automaticamente dalla Piattaforma.

5.2. Descrizione della funzionalita' per l'esposizione delle informazioni relative alla sottoscrizione al cittadino (art. 5, co. 4 del decreto)

Le informazioni anagrafiche insieme all'ID sessione sono esposte al cittadino in relazione all'iniziativa che intende sottoscrivere selezionando l'apposito tasto che lo invita alla sottoscrizione.

La sottoscrizione da parte del cittadino si realizza con due azioni consecutive compiute dallo stesso: selezione del pulsante che invita alla sottoscrizione con apertura dell'anteprima del documento e nuova selezione sulla conferma.

5.3. Descrizione della funzionalita' per la certificazione del processo di sottoscrizione da parte del gestore (art. 5, co. 6 del decreto)

Le operazioni realizzate dal cittadino sono registrate e archiviate insieme alle informazioni anagrafiche e all'ID sessione e sono collegate al documento informatico relativo all'iniziativa tramite hash generato come da funzionalita' descritta al paragrafo 4.3.

La certificazione del processo descritto e' garantita dall'apposizione, sull'attestazione di sottoscrizione, del Sigillo elettronico qualificato del gestore.

5.4. Modalita' di accesso del cittadino ai dati relativi alle proprie sottoscrizioni (art. 6, co. 4 del decreto)

L'attestato di sottoscrizione che il cittadino puo' scaricare utilizzando gli strumenti di gestione della sottoscrizione, riporta, oltre ai dati anagrafici, l'identificativo univoco della sessione utente avviata tramite autenticazione verso un IDP esterno (SPID, CIE, CNS) e il riferimento all'iniziativa sottoscritta sia testuale che tramite hash.

I cittadini potranno visualizzare le proprie sottoscrizioni effettuate accedendo all'area privata del portale.

6. Gestione della messa a disposizione delle sottoscrizioni raccolte

Le evidenze informatiche relative alla raccolta delle sottoscrizioni vengono esposte ai profili abilitati in diverse modalita':

1. direttamente sul portale con possibilita' di ricerca, accesso, estrazione e verifica dei singoli documenti informatici generati a seguito di sottoscrizione;

2. tramite elenchi periodicamente generati dalla piattaforma, suddivisi per comune di iscrizione nelle liste elettorali, sia in formato pdf munito di sigillo elettronico qualificato che in formato csv contenenti i seguenti dati:

Titolo del quesito referendario/iniziativa popolare

Codice fiscale

Nome, cognome, data di nascita, luogo di nascita

Timestamp della sottoscrizione

Comune di iscrizione nelle liste elettorali dichiarato (o confermato a seguito di chiusura della raccolta delle sottoscrizioni - si veda il successivo paragrafo 6.3).

6.1. Descrizione della funzionalita' per terminare la raccolta delle sottoscrizioni da parte dei promotori (art. 4, co. 8 del decreto)

La piattaforma chiude automaticamente la raccolta delle sottoscrizioni secondo le tempistiche previste dalle norme per la specifica tipologia di iniziativa. L'utente promotore attraverso gli strumenti di gestione dell'iniziativa puo' anche interrompere in qualsiasi momento la raccolta delle sottoscrizioni.

La chiusura dell'iniziativa alla raccolta delle sottoscrizioni rendera' la stessa definitivamente chiusa e non ne sara' possibile la riapertura.

6.2. Descrizione della funzionalita' per la richiesta di certificazione elettorale al comune (art. 4, co. 10 del decreto)

Fino all'integrazione delle liste elettorali nel sistema ANPR, attraverso gli strumenti di gestione dell'iniziativa, l'utente promotore, dopo la chiusura delle sottoscrizioni, genera un messaggio di PEC per ogni comune per il quale risultano cittadini sottoscrittori dell'iniziativa con la richiesta di verifica dell'iscrizione dei sottoscrittori nelle liste elettorali e di rilascio del relativo certificato. La piattaforma provvede in automatico all'invio dei messaggi cosi' generati alle caselle PEC dei comuni estratte dall'Indice dei domicili digitali della pubblica amministrazione e dei gestori di pubblici servizi, di cui all'art. 6 ter del CAD, ed alla gestione delle ricevute di accettazione e di avvenuta consegna di cui all'art. 6 del decreto del Presidente della Repubblica 11 febbraio 20015, n. 68. Le ricevute sono consultabili secondo quanto specificato al paragrafo 7.1.1.

6.3. Descrizione della funzionalita' per la messa a disposizione delle sottoscrizioni e delle relative evidenze informatiche da parte dei promotori all'Ufficio Referendum (art. 7, co. 1 del decreto)

L'utente promotore, tramite gli strumenti di gestione dell'iniziativa, selezionando l'apposito tasto, mette a disposizione della Corte di cassazione gli elenchi prodotti dalla piattaforma dopo l'invio della richiesta di verifica dell'iscrizione nelle liste elettorali dei cittadini sottoscrittori ai comuni competenti tramite PEC ovvero nel momento della verifica dell'attributo elettore in ANPR.

6.4. Descrizione della funzionalita' per la messa a disposizione dei promotori dell'attestazione di messa a disposizione delle sottoscrizioni alla Corte di cassazione (art. 7, co. 2 del decreto)

L'utente promotore, dopo la messa a disposizione degli elenchi, puo' utilizzare gli strumenti di gestione dell'iniziativa per scaricare l'attestato di messa a disposizione e gli elenchi delle sottoscrizioni in formato pdf, muniti di Sigillo elettronico nonche' di marca temporale.

6.5. Descrizione delle funzionalita' di estrazione del duplicato informatico e della copia analogica per le proposte di legge di iniziativa popolare (art. 7, co. 5 del decreto)

Tutti i documenti informatici generati dalla piattaforma in formato pdf muniti di sigillo elettronico e/o di marca temporale possono essere estratti quale duplicato informatico e sono muniti di contrassegno ai sensi dell'art. 23, comma 2 bis, del CAD ai fini della loro verifica per l'eventuale copia analogica prodotta.

7. Accesso alle sottoscrizioni

7.1. Descrizione della funzionalita' per la verifica delle firme da parte della Corte di cassazione (art. 7, co. 3 del decreto)

Successivamente alla messa a disposizione delle sottoscrizioni da parte dei promotori, gli utenti della Corte di cassazione (profilo magistrato eventualmente coadiuvato da altri profili che possono autorizzare ai sensi del decreto), attraverso gli strumenti di gestione della piattaforma, possono visualizzare, anche secondo ordinamenti personalizzati, l'elenco di tutte le sottoscrizioni effettuate dai cittadini complete dei relativi dati, nonche' ricercare e selezionare una o piu' sottoscrizioni per la verifica puntuale internamente o, previa estrazione, esternamente alla piattaforma.

7.1.1. Descrizione della funzionalita' di accesso alle sottoscrizioni e relative evidenze informatiche da parte dell'utenza «cassazione» (art. 6, co. 2 del decreto)

Gli utenti della Corte di cassazione hanno altresi' accesso ai documenti informatici relativi all'iniziativa nonche' a tutte le evidenze informatiche generate in relazione alla stessa e possono estrarli per i relativi controlli.

7.2. Descrizione della funzionalita' di estrazione dati da parte degli utenti della Corte di cassazione per controllo duplicazione sottoscrizioni (art. 7, co. 7 del decreto)

Successivamente alla messa a disposizione delle sottoscrizioni da parte dei promotori, gli utenti della Corte di cassazione (profilo magistrato eventualmente coadiuvato da altri profili che possono autorizzare ai sensi del decreto), attraverso gli strumenti di gestione della piattaforma, possono estrarre, anche secondo ordinamenti personalizzati, gli elenchi sia in formato pdf munito di

sigillo elettronico e marca temporale, che in formato lavorabile.

8. Descrizione delle caratteristiche tecniche, regole tecniche e requisiti di sicurezza della piattaforma (art. 3, co. 3, del decreto)

8.1. Sicurezza perimetrale e di rete

Tutto il traffico diretto al servizio attraversa le infrastrutture di sicurezza esterne dei data center (DDoS Protector, IPS e Firewall) ed e' poi inoltrato alla prima struttura di bilanciamento. Tale struttura procede al Proxy (Source NAT) delle connessioni eliminando l'indirizzo IP pubblico e inoltrando con il proprio indirizzo tutte le connessioni ai sistemi posizionati in DMZ. I sistemi di bilanciamento non tracciano le connessioni.

I sistemi posizionati in DMZ provvedono ad una analisi iniziale del traffico e, laddove previsto, eliminano la componente dummy e trasferiscono al backend le chiamate residue.

Il successivo strato di sicurezza e' posto tra i sistemi in DMZ della infrastruttura e i server di backend a protezione di questi ultimi (Firewall, Bilanciatore/WAF e IPS).

Il backend e' poi realizzato all'interno di un cluster di server virtuali, su cui e' implementato un modello di sicurezza infrastrutturale a microsegmentazione.

Le infrastrutture di sicurezza perimetrale esterne sono realizzate in sequenza attraverso i seguenti dispositivi, in livelli successivi:

DDoS Protector: e' un dispositivo esposto sulla frontiera piu' esterna della rete Internet per mitigare eventuali attacchi mirati a rendere il servizio indisponibile (es. DoS e DDoS), sia di tipo volumetrico che qualitativi. Nello specifico, il dispositivo e' connesso in modalita' Layer2 tra i router esterni e i firewall perimetrali, lavorando in collaborazione con l'analogo servizio erogato dagli Internet Service Provider. Rileva dinamicamente e blocca eventuali tentativi di attacco (sono registrati gli indirizzi IP pubblici e relativi eventi attinenti tentativi di attacco riconosciuti).

Sonde di Network Intrusion Prevention (NIPS): i dispositivi hanno il compito di mitigare gli attacchi diretti ai server di frontend che erogano i servizi web; nello specifico sono interconnesse in modalita' Layer 2 tra i router esterni e i firewall perimetrali.

Firewall di perimetro che autorizzano le comunicazioni verso le reti e i sistemi attestati sulla DMZ e il back-end, attuando controlli delle sessioni (Stateful Inspection) e dei protocolli applicativi autorizzati (Protocol Enforcement).

Un ulteriore strato di sicurezza e' posto tra i sistemi in DMZ della infrastruttura e i server di backend. Tale infrastruttura e' composta da firewall che separano la rete DMZ dalla rete dove e' posizionato il backend e da un ulteriore strato di bilanciamento comprensivo di funzionalita' Web Application Firewall (WAF) e di Sonde NIPS poste a protezione dei sistemi di backend.

Il sistema WAF introduce inoltre uno strato di sicurezza di tipo Signature-Based, che viene successivamente supportato da ulteriori dispositivi di Network Intrusion Prevention, presenti nella infrastruttura di rete e configurati in modalita' Layer 2. L'utilizzo di sessioni applicative crittografate (HTTPS TLS 1.2+) richiede l'utilizzo della modalita' operativa denominata SSL End to End, necessaria per la decrittazione del traffico, l'analisi e il blocco di eventuali attacchi applicativi come ad esempio Cross-Site Scripting (XSS), SQL injection, ecc. Sono registrate dal dispositivo esclusivamente le connessioni provenienti dall'indirizzo IP privato dei server in DMZ, inerenti a tentativi di attacchi applicativi.

Le regole di sicurezza applicate al sistema WAF sono strettamente legate alle funzionalita' dei servizi erogati e sono impostate successivamente a una fase iniziale detta di learning, in cui il dispositivo apprende il funzionamento lecito dell'applicazione.

In generale i gruppi di servizi, gli utenti e i sistemi informativi sono sempre segmentati a livello di rete.

L'accesso agli strumenti di configurazione degli apparati di rete e' consentito solo a personale inserito in specifici gruppi di utenza, gli unici ad avere una profilatura di massimo livello delle chiavi di accesso agli apparati. Oltre all'inserimento delle

credenziali di accesso personali, viene effettuato un ulteriore controllo a livello di MAC address (layer 2) o di IP address (layer 3). Solo i MAC o gli IP address delle postazioni associate al personale autorizzato sono presenti in una white-list di MAC o IP address tenuta costantemente aggiornata, e distribuita su tutti gli apparati di rete. In tal modo si permette l'accesso alle risorse (sia tramite CLI che tramite GUI) solo da tali postazioni, e solo dal personale autorizzato. Inoltre, tutte le operazioni effettuate sugli apparati di rete sono registrate e storicizzate da apposito e diverso gruppo di monitoraggio.

Tutte le porte non utilizzate degli apparati di rete vengono lasciate esplicitamente disabilitate finche' non si rende necessaria una loro configurazione e successivo utilizzo, a seguito di specifica richiesta utente o di specifico progetto.

8.2. Controllo accessi

L'accesso alla piattaforma del referendum e' effettuato tramite SPID, CIE o CNS.

8.3. Sicurezza fisica

L'accesso alle sedi aziendali del gestore della piattaforma e' controllato da un servizio di vigilanza armata della Guardia di Finanza con presenza 24 ore su 24, da dispositivi di registrazione degli accessi supportati da tornelli, che costituiscono anche una barriera fisica, da sistemi di videosorveglianza a circuito' chiuso (TVCC) e da un servizio di ronda notturna, anch'esso di responsabilita' della Guardia di Finanza.

Inoltre, la sede centrale, dove sono installate le infrastrutture tecniche (hardware e software) e logistiche, e' circondata da un muro di cinta in cemento armato, sormontato da una recinzione, dotato di barriera a fili tesi anti intrusione e provvisto di sonde anti sfondamento.

Al fine di innalzare il livello di sicurezza all'interno della sala CED, posta al piano interrato, e' presente un presidio permanente della Guardia di Finanza e un accesso fisico controllato con tornelli ed attivo tramite badge al solo personale autorizzato. E' inoltre installato all'interno un sistema di telecamere a circuito chiuso.

Tutte le telecamere del sistema di videosorveglianza perimetrale e del CED, configurato in alta affidabilita', sono asservite a videoregistratori, posti in un'apposita sala regia governata 24 ore su 24 dalla Guardia di Finanza, dove fanno capo anche le segnalazioni provenienti dai sistemi anti intrusione e anti sfondamento.

L'accesso fisico alle sedi aziendali, regolato da norme specifiche, e' consentito soltanto al personale autorizzato. In particolare, le modalita' di accesso alle sedi sono diversificate per persone, materiali ed automezzi.

I server che implementano le applicazioni ed i servizi di backend del progetto risiedono in sala CED all'interno di armadi rack metallici chiusi.

8.4. Conduzione operativa

8.4.1. Disaster recovery

Le modalita' adottate per effettuare la replica vanno dall'utilizzo delle tecniche di replica array-based del sottosistema storage che contiene i dati e gli ambienti interessati fino alla replica remota delle copie di salvataggio effettuate tramite le procedure di backup, attivando la replica tra i sottosistemi a disco che contengono le copie di backup.

L'RPO (Recovery Point Objective) garantito nel caso di replica array-based e' inferiore al minuto, nel caso della replica dei backup puo' essere dell'ordine di poche decine di minuti (per backup incrementali degli archive log dei database) o di un tempo piu' lungo che dipende dall'ultimo backup full effettuato con successo.

In entrambi i casi l'RTO (Recovery Time Objective) garantito per il servizio di disaster recovery adottato e' dell'ordine di I settimana.

Per il servizio ICT viene effettuata la replica array-based dei seguenti elementi:

- dati
- sistemi operativi e configurazioni ambienti virtuali

La replica adottata e' continua e non prevede fermi durante le

simulazioni di ripartenza sul sito secondario.

Le operazioni di replica sono costantemente monitorate e nel caso di fermo accidentale possono essere riattivate senza perdita dei dati gia' replicati e ripartendo, con l'adozione di tecniche di journaling, dal punto di interruzione avvenuto.

La replica del backup avviene tra due sottosistemi a disco su cui sono depositati i backup effettuati, la replica avviene per differenze basandosi sulla funzionalita' di deduplica del sottosistema.

8.4.2. Vulnerabilita' tecniche e patching

L'aggiornamento (patching) dei sistemi informatici viene effettuato con cadenza almeno semestrale secondo la seguente procedura:

si valutano e si documentano i rischi connessi alle vulnerabilita' esistenti e agli impatti negativi che si potrebbero avere sulla funzionalita' (es. incompatibilita')

si definiscono gli eventuali piani di rientro laddove non sia possibile eseguire l'aggiornamento

si eseguono e si documentano le procedure secondo il piano di test predefinito

Le patch e gli aggiornamenti software, per il sistema operativo e per le applicazioni, vengono installate mediante procedure automatizzate.

Le attivita' di verifica delle vulnerabilita' (vulnerability assessment) di un servizio ICT sono svolte attraverso strumenti costantemente aggiornati rispetto agli ultimi vettori di attacco scoperti e seguono specifici test-plan definiti in base alla documentazione di progetto ed alla tipologia di piattaforma, con un processo strutturato che prevede:

la rilevazione del perimetro d'intervento

la rilevazione e la classificazione delle vulnerabilita'/non conformita' l'individuazione del possibile impatto

la comunicazione dei risultati ai responsabili di sistema

la definizione dei piani di rientro con i relativi interventi tecnici

il monitoraggio periodico delle attivita' precedenti

Tali attivita' sono pianificate in funzione della criticita' dei sistemi impattati e risultano oggettive, ripetibili e conformi agli standard di riferimento (es. CVE).

8.4.3. Penetration test

Sono previste attivita' di Penetration Test sui vari servizi applicativi coinvolti nell'architettura, tra cui i vari servizi web esposti. Tali attivita' sono svolte a cura di un team dedicato, specializzato nell'analisi delle applicazioni. Le attivita' vengono realizzate di norma in fase di pre-rilascio, su ambienti consolidati, ma possono essere previste anche su base sistematica e continuativa.

I test sono volti ad individuare vulnerabilita' applicative ed infrastrutturali che possono comportare un utilizzo non corretto e potenzialmente dannoso dei servizi, ad evitare eventuali accessi non autorizzati, abusi o usi impropri delle applicazioni, nonche' eventuali esposizioni di informazioni riservate (data leakage). Ogni test di sicurezza permette di produrre un report di dettaglio sulle vulnerabilita' individuate, comprensivo di esemplificazioni delle opzioni di sfruttamento - che escludono i falsi positivi - nonche' i riferimenti per indirizzarne una efficace mitigazione.

La verifica dell'effettiva risoluzione delle segnalazioni puo' essere effettuata successivamente con retest mirati.

I test sono di norma eseguiti sull'ambiente di validazione, a valle del deploy effettuato dalle pipeline di Cl/CD, su una versione del software consolidata e congruente rispetto alla versione in rilascio.

Oltre ai test dinamici, eseguiti sui servizi applicativi in esecuzione e funzionanti, sono eseguiti test statici di sicurezza tramite l'analisi del codice sorgente dei servizi stessi e delle immagini generate a valle del processo di Cl/CD. L'analisi statica ha l'obiettivo di valutare la sicurezza, la qualita' del codice ed eventuali vulnerabilita' presenti nelle librerie applicative di terze parti utilizzate.

Tutte le verifiche di sicurezza, dinamiche e statiche, nonche' la

classificazione delle vulnerabilita', sono basate sulla metodologia OWASP - Open Web Application Security Project, Standard di riferimento internazionale per la sicurezza delle applicazioni web.

8.4.4. Benchmark

Prima del rilascio di ogni servizio in produzione, a fronte di uno studio di capacity, si verifica che il target prefissato di transazioni al secondo venga raggiunto nel rispetto dei tempi di risposta previsti, simulando i principali scenari d'uso dell'applicazione. Gli script realizzati per l'esecuzione dei test vengono inoltre raccolti e manutenuti in un repository centrale in modo da riutilizzarli per successive release del servizio, dopo aver effettuato gli opportuni aggiornamenti.

8.5. Sicurezza cibernetica

8.5.1. Benchmark

Prima del rilascio di ogni servizio in produzione il team dedicato alla progettazione ed esecuzione di test di carico, a fronte di uno studio di capacity, verifica che il target prefissato di transazioni al secondo venga raggiunto nel rispetto dei tempi di risposta previsti, simulando i principali scenari d'uso dell'applicazione. Gli script realizzati per l'esecuzione dei test vengono inoltre raccolti e manutenuti in un repository centrale in modo da riutilizzarli per successive release del servizio, dopo aver effettuato gli opportuni aggiornamenti.

8.5.2. Procedure di risposta agli incidenti

Il gestore della piattaforma dispone di una procedura aziendale che definisce processi, ruoli, compiti ed attivita' per quanto riguarda le azioni di risposta agli incidenti di sicurezza. La procedura e' stata strutturata per essere pienamente GDPR-compliant, e pone un focus particolare alla gestione di incidenti che coinvolgono violazioni di dati personali (data breach), con attenzione circa le tempistiche di notifica al titolare previste dalla normativa.

La procedura dettaglia i ruoli di ogni struttura aziendale impattata, sia internamente che verso i clienti-titolari, ed e' costantemente aggiornata per includere tutte le modifiche agli attori aziendali coinvolti nel processo di gestione dell'incidente.

8.5.3. Scenari di attacco

L'utente accede alla piattaforma referendum tramite SPID, CIE o CNS con identita' fornita dall'Identity Provider usato nel processo di autenticazione. Al Provider spetta la fase di identificazione ed autenticazione gli utenti e la propagazione dell'identita' dell'utente al servizio.

Nel caso in cui uno degli apparati di sicurezza presenti nell'infrastruttura identificasse attivita' non lecita, riconducibile ad attacchi noti di Cross-Site Scripting (XSS), SQL injection, ecc., si potra' rilevare l'utente loggato in sessione e bloccare le richieste malevoli.

In alcuni casi specifici, nel caso in cui l'attivita' malevola risultasse insistente, gli apparati di sicurezza possono essere configurati per inibire/bloccare temporaneamente la sessione di lavoro.

8.5.4. Interruzione dei servizio

L'interruzione del servizio puo' essere ottenuta compromettendo e rendendo inefficace una componente del servizio stesso, impedendo il funzionamento o sovraccaricando un elemento tanto da renderlo inservibile.

L'interruzione del servizio puo' essere il risultato di attivita' esterne all'infrastruttura come interne all'infrastruttura.

L'interruzione del servizio compromette la disponibilita' dei dati.

8.5.5. Intercettazione delle comunicazioni e intromissione

L'intercettazione delle comunicazioni puo' essere attuata al di fuori dell'infrastruttura, compromettendo un elemento coinvolto nella trasmissione delle comunicazioni, oppure all'interno dell'infrastruttura accedendo ai dati oggetto della comunicazione.

Anche in caso di misure di sicurezza presenti, quali cifratura e offuscamento, l'intercettazione puo' portare alla compromissione di comunicazioni protette. In questo caso, la protezione deve essere violata per permettere all'attaccante l'accesso alle comunicazioni.

L'intercettazione delle comunicazioni e l'intromissione compromettono la riservatezza dei dati.

8.5.6. Violazione della integrita' delle comunicazioni

La violazione dell'integrita' delle comunicazioni avviene quando un attaccante acquisisce l'accesso alle informazioni ed e' in grado di alterarle, cancellarle o crearne di nuove. La violazione puo' avvenire se le difese in essere sono superate o aggirate e l'attaccante ha l'opportunita' di accedere ai dati.

La violazione dell'integrita' delle comunicazioni impatta chiaramente l'integrita' dei dati.

8.5.7. Identificazione delle vulnerabilita' applicative

La pubblicazione del codice sorgente, anche se verificato tramite penetration test (vedi paragrafi precedenti) alza necessariamente l'attenzione circa le modalita' di funzionamento delle applicazioni e di conseguenza l'identificazione di vulnerabilita' nel codice.

Analogo discorso e' applicabile per le librerie e tecnologie usate che vanno analizzate laddove possibile e comunque aggiornate qualora dal monitoraggio della pubblicazione di specifici bollettini emergano possibili criticita'.

8.6. Misure di monitoraggio

8.6.1. Monitoraggio sistemi di sicurezza

I sistemi di sicurezza perimetrale a protezione dell'infrastruttura di erogazione del servizio sono costantemente monitorati tramite strumenti di raccolta e correlazione log provenienti dagli apparati (SIEM). Il Security Operation Center del gestore della piattaforma opera su diversi livelli di intervento, garantendo un monitoraggio 24/7 di tutti i sistemi, e la gestione di problematiche, sia tecniche che derivanti da possibili attacchi, e' inserita e regolata dalla procedura aziendale di gestione degli incidenti descritta in precedenza.

Sono altresi' previste specifiche Incident Response Procedure (IRP) per gli operatori che svolgono il monitoraggio al fine di rispondere tempestivamente alle problematiche emerse, attuando una risposta immediata e attivando le procedure di escalation verso gli altri livelli di gestione dell'evento, se necessarie.

Le IRP prevedono infatti, in conformita' con le procedure aziendali, l'immediata identificazione (triage) del livello di minaccia al servizio e l'adozione di adeguate contromisure di risposta.

8.6.2. Monitoraggio OSINT

Il gestore della piattaforma, tramite il CERT, opera un continuo monitoraggio di fonti OSINT (Open Source INTelligence), al fine di individuare, con la massima efficienza, indicatori di compromissione (IoC) e/o vulnerabilita' collegati ai servizi erogati. Per ogni monitoraggio, viene predisposto un pacchetto di dati tecnici di interesse, che vengono ricercati e controllati sulle fonti disponibili in maniera «aperta», a titolo di esempio siti web, social network, piattaforme di condivisione, community specifiche, forum, ecc,

La rilevazione di un elemento di interesse (IoC o vulnerabilita') fra le fonti controllate, porta alla sua contestualizzazione, analisi e valutazione, anche sulla base dell'affidabilita' della sorgente informativa, al fine di applicare un criterio di prioritizzazione e determinare le opportune contromisure, indirizzandole verso i gruppi di competenza.

8.7. Tracciamento

Il gestore della piattaforma dispone di sistemi di tracciamento dei servizi che ospita e gestisce, sia dal punto di vista applicativo (cioe' il tracciamento dell'uso del servizio stesso), sia relativamente ai sistemi informatici di supporto come database, server web e infrastrutture a supporto del servizio.

Nello specifico per ogni accesso alle basi dati ospitate presso i CED, effettuato tramite utenze nominali o riconducibili ad una persona fisica (escluse le utenze di servizio), il sistema di tracciamento DB registra (su appositi log) le seguenti informazioni:

- identificativo univoco dell'utenza che accede;
- data e ora di login, logout e login falliti;
- postazione di lavoro utilizzata per l'accesso (indirizzo IP del client);

tipo di operazione eseguita sui dati (ad esclusione delle risposte alle query).

Per ogni accesso ai sistemi operativi, ai sistemi di rete, e ai sistemi di sicurezza, il sistema di tracciamento degli accessi degli Amministratori di Sistema registra (su appositi log) le seguenti informazioni:

identificativo univoco dell'utenza che accede;

data e ora di login, logout;

postazione di lavoro utilizzata per l'accesso (indirizzo IP del client).

In aggiunta a cio' il sistema traccia le seguenti informazioni:

sui firewall, qualsiasi operazione effettuata dagli amministratori di sistema (ambito firewall) su apposito log (separato dai normali log delle regole); il log in questione e' in formato proprietario, cifrato e disponibile solo con apposita console anche essa ad accesso strettamente limitato

sui sistemi di rete, qualsiasi operazione effettuata dagli amministratori di sistema (ambito rete)

sui sistemi operativi, le motivazioni dell'accesso degli amministratori di sistema

I log prodotti dai sistemi di tracciamento infrastrutturali sono soggetti a monitoraggio costante allo scopo di individuare eventuali anomalie inerenti alla sicurezza (accessi anomali, operazioni anomale, ecc.) e di valutare l'efficacia delle misure implementate.

I log di accesso degli Amministratori di sistema e degli incaricati sono protetti da eventuali tentativi di alterazione e dispongono di un sistema di verifica della loro integrita'.

I log relativi agli accessi e alle operazioni effettuate sui dati, sui sistemi operativi, sulla rete, sul software di base e sui sistemi complessi in produzione sono conservati per dodici mesi.

8.8. Capacita' dell'infrastruttura

Il gestore della piattaforma dispone di procedure e processi di change management che tengono traccia di tutte le richieste di variazione sui vari servizi, dalla fase di startup fino alle operazioni di adeguamento della capacita' dell'infrastruttura. Le componenti hardware/software del servizio sono censite su un sistema CMDB (Change Management DataBase).

Il servizio e' sottoposto a monitoraggio continuo della capacita', tramite strumenti di analisi che osservano i seguenti parametri:

performance della rete (utilizzo di banda);

utilizzo di CPU;

occupazione della RAM;

occupazione del file system;

spazio disco utilizzato e disponibile.

Laddove i sistemi di monitoraggio indicano come necessario un adeguamento di capacita' dell'infrastruttura tecnologica a supporto del servizio viene redatto, secondo le procedure aziendali, un piano di adeguamento tecnologico che contiene:

l'analisi effettuata sul monitoraggio del servizio;

le variazioni da implementare per raggiungere i risultati desiderati sui componenti dell'infrastruttura interessati agli interventi;

l'orizzonte temporale in cui effettuare le modifiche.

8.9. Continuita' del servizio

Il gestore della piattaforma, per garantire un migliore livello di affidabilita' dei servizi offerti, adotta un modello di strutturazione dell'infrastruttura all'interno del CED che prevede la duplicazione di tutte le componenti hardware, con una collocazione in zone del CED separate nelle quali tutta la catena degli elementi logistici (alimentazione, quadri, raffreddamento, armadi, etc.) risulti indipendente.

Questa struttura, unita alle caratteristiche di alta affidabilita' delle componenti software utilizzate, garantisce la continuita' di servizio per i sistemi attestati nei CED.

8.10. Servizi sistemistici e gestionali per la conduzione, il controllo e il mantenimento in efficienza dell'infrastruttura

L'infrastruttura tecnologica del gestore della piattaforma viene costantemente monitorata dal personale di conduzione per garantirne

la continuita' operativa, l'efficienza e la naturale evoluzione.

Questa attivita' si inquadra nell'ambito di alcuni processi conformi allo standard ITIL che annoverano l'Incident Management, il Problem Management, l'Availability Management, il Service Continuity Management ed il Release and Deployment Management.

Con tali processi vengono garantite, attraverso opportuni monitoraggi sia infrastrutturali che di servizi erogati (precedentemente descritti), l'intervento sia proattivo che reattivo nel caso si manifestassero dei problemi che riducessero l'efficacia operativa di questi ultimi.

L'approccio identificato in questi processi aziendali e' affine ai concetti di DevOps, per i quali il personale dedicato alla gestione della conduzione dei servizi stabilisce interazioni con i gruppi di sviluppo software sia nella fase di implementazione che nelle modifiche al servizio e nella risoluzione di eventuali problematiche.

8.11. Monitoraggio dell'infrastruttura, del servizio e delle performance

Nell'ambito dei processi del gestore della piattaforma su standard ITIL, il monitoraggio del servizio con focus sull'Incident Management e' svolto tramite la struttura di First Line Support (FLS).

Il team, in presenza 24/7 presso la sede del gestore della piattaforma, svolge una verifica della disponibilita' e continuita' dei sistemi e dei servizi, mediante la realizzazione di molteplici controlli che generano segnalazioni di allarmi alle console centralizzate, monitora l'attivazione di azioni automatiche di ripristino e interviene con specifiche procedure operative laddove necessario.

Al fme di ottimizzare il processo, si e' adottato e' sviluppato un modello di controllo di tipo Service Control Room che, basandosi sulle informazioni contenute nel CMDB (descritto in precedenza) riesce a mappare l'infrastruttura tecnologica sui servizi offerti agli utenti, arricchendo con i pesi relativi all'impatto gli allarmi provenienti dai controlli sulle tecnologie.

I controlli realizzati sono specifici a seconda della piattaforma tecnologica utilizzata.

8.12. Trattamento dei dati personali

Il trattamento dei dati personali oggetto del presente manuale e' stato sottoposto a valutazione d'impatto ai sensi dell'art. 35 del Regolamento (UE) 2016/679 che individua puntualmente le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali.

In particolare, la piattaforma adotta misure, atte a garantire l'integrita' e la riservatezza dei dati scambiati e conservati, la sicurezza dell'accesso ai servizi, il tracciamento delle operazioni effettuate.

Per garantire l'autenticazione, l'integrita' e la riservatezza in senso crittografico dei dati, la piattaforma utilizza il protocollo di comunicazione HTTPS (HTTP over TLS).

La versione del protocollo TLS e le cipher suite utilizzate sono la versione 1.2 o superiore.

Periodicamente e ad ogni nuova release il sistema e' sottoposto a Web Application Penetration Test, per la verifica della presenza di eventuali vulnerabilita'.

Tutti i sistemi afferenti alla piattaforma sono sottoposti ad «hardening».

Il gestore della piattaforma ha adottato tutte le iniziative necessarie per il mantenimento di un'alta qualita' del servizio (QoS, Quality of Service), utilizzando buone pratiche, ad esempio, per assicurare prestazioni e scalabilita' e per il risparmio della banda.

Come strumento di misura della QoS, il gestore della piattaforma e' soggetto a quelli che vengono definiti Service Level Agreement (SLA), ovvero accordi sul livello di servizio.

8.13. Descrizione delle metriche di successo e fallimento delle operazioni eseguite, unitamente a metriche prestazionali e di qualita', nonche' di assistenza agli utenti per monitorare l'operativita' della piattaforma (art. 3, co. 3, del decreto)

La piattaforma raccoglie metriche applicative dei vari servizi, permettendo cosi' il controllo continuo della piattaforma sia in termini di disponibilita', di traffico (throughput) e di tempi di risposta. Questi dati saranno presentati in forma grafica (dashboard) alle unita' organizzative del gestore adibite al monitoraggio, in modo che possano essere prese azioni immediate a fronte di incident atte al ripristino immediato del sistema. Le specifiche di dettaglio di tali metriche saranno pubblicate sul portale della piattaforma, nella sezione dedicata.

La piattaforma, oltre ad integrare meccanismi di logging interni, si connette ad API esterne per la raccolta (log collection), la ricerca e la produzione di analitiche, utili tra l'altro all'identificazione di problemi e al monitoraggio del sistema e della QoS.

Il gestore traccia un evento per ogni richiesta, contenente almeno i seguenti parametri minimi:

- istante della richiesta;
- identificativo del fruitore e dell'operazione richiesta;
- tipologia di chiamata;
- esito della chiamata;
- ove applicabile, un identificativo univoco della richiesta, utile a eventuali correlazioni.

8.14. Modalita' comunicazione data breach da parte del gestore (art. 9, co. 7 del decreto)

La piattaforma garantisce ai titolari del trattamento competenti la conoscenza, in maniera tempestiva, delle violazioni di sicurezza o di qualsiasi minaccia che comporti un rischio per la sicurezza e per i diritti e le liberta' degli interessati al trattamento tramite notifica sul portale e tramite gli indirizzi elettronici di riferimento inseriti nei profili dell'iniziativa nonche' tramite canale dedicato nei confronti della Corte di cassazione.