Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

DETERMINAZIONE COMMISSARIALE N.168/2013 DIG

OGGETTO: MODALITÀ DI PRESENTAZIONE DELLA DOMANDA PER LA CERTIFICAZIONE DEI SISTEMI DI RACCOLTA ELETTRONICA PER LE INIZIATIVE DEI CITTADINI EUROPEI – APPLICAZIONE DEL REGOLAMENTO (UE) N. 211/2011.

IL DIRETTORE GENERALE IN QUALITA' DI COMMISSARIO STRAORDINARIO

VISTO il decreto legislativo 1° dicembre 2009, n. 177 recante "*Riorganizzazione del Centro nazionale per l'informatica nella pubblica amministrazione, a norma dell'articolo 24 della legge 18 giugno 2009, n. 69*" e successive modifiche e integrazioni;
VISTI gli articoli 19 (*Istituzione dell'Agenzia per l'Italia Digitale*), 20 (*Funzioni*), 21(*Organi e Statuto*) e 22 (*Soppressione di DigitPA e dell'Agenzia per la diffusione delle tecnologie per l'innovazione; successione dei rapporti e individuazione delle effettive risorse umane e strumentali*) del decreto legge n. 83 del 22 giugno 2012, recante *"Misure urgenti per la crescita del Paese"*, convertito, con modificazioni, nella legge 7 agosto 2012, n. 134 nei relativi testi come modificati dall'art. 13, comma 2, del decreto legge n.69 del 21 giugno 2013 convertito in legge 9 agosto 2013 n. 98;
VISTO, in particolare, il comma 2, dell'art. 22, del citato decreto legge n. 83/2012 che prevede, tra l'altro, che "*... il Direttore Generale esercita in via transitoria le funzioni svolte dagli Enti soppressi e dal Dipartimento di cui all'art. 20, comma 2, in qualità di Commissario straordinario, fino alla nomina degli altri organi dell'Agenzia per l'Italia Digitale*";
VISTO il decreto del Presidente del Consiglio dei Ministri in data 30 ottobre 2012, registrato dalla Corte dei Conti il 20 dicembre 2012, con il quale l'Ing. Agostino Ragosa è stato nominato, per la durata di un triennio, Direttore Generale dell'Agenzia per l'Italia Digitale;
VISTO il regolamento (UE) n. 211/2011, del Parlamento europeo e del Consiglio, del 16 febbraio 2011, riguardante l'iniziativa dei cittadini;
VISTO il regolamento di esecuzione (UE) n. 1179 - della Commissione, del 17 novembre 2011, che fissa le specifiche tecniche per i sistemi di raccolta per via elettronica a norma del regolamento (UE) n. 211/2011 riguardante l'iniziativa dei cittadini;
TENUTO CONTO dell'apertura del caso EU pilot 3863/12/SGEN – Applicazione del Regolamento n. 211/2011;
VISTA la pubblicazione del Decreto del Presidente della Repubblica 18 ottobre 2012, n. 193 – "Regolamento concernente le modalità di attuazione del regolamento (UE) n. 211/2011 riguardante l'iniziativa dei cittadini. (12G0214)", pubblicata in GU n. 267 del 15-11-2012 (testo in vigore dal: 30-11-2012)
RICONOSCIUTO che tra le funzioni istituzionali attribuite alla Agenzia per l'Italia Digitale rientra quella disciplinata dall'art. 4 del Decreto del Presidente della Repubblica 18 ottobre 2012, n. 193, di emanazione del regolamento concernente le modalità di attuazione del regolamento (UE) n.211/2011 riguardante l'iniziativa dei cittadini;
CONSIDERATO che, ai sensi dell'art. 4 del sopra citato DPR n. 193/2012, l'Agenzia per l'Italia Digitale è autorità competente per la certificazione dei sistemi di raccolta elettronica di cui all'art 6 regolamento (UE) n. 211/2011, del Parlamento europeo e del Consiglio e individua,

entro 15 giorni dalla data di entrata in vigore dello stesso regolamento, (ossia entro il 15 dicembre 2012) con propria deliberazione la documentazione da depositare e le modalità per presentare domanda per la certificazione dei sistemi di raccolta elettronica;

RICORDATO che con deliberazione n. 30 del 29 novembre 2012 il Comitato Direttivo del soppresso DigitPA ha approvato la procedura per il rilascio della certificazione e della attestazione di conformità dei sistemi di raccolta per via elettronica per l'iniziativa dei cittadini europei, in attuazione del citato 4 del regolamento di cui al DPR n. 193/2012;

CONSIDERATO che con nota pervenuta in data 28 marzo 2013 (prot. AgID 2356) il Capo Dipartimento per le Politiche Europee della Presidenza del Consiglio dei Ministri – Struttura di missione per le procedure di infrazione – ha comunicato che il competente servizio della Commissione europea ha accettato la risposta fornita dalle Autorità italiane con nota DPE prot. 1661 del 6/3/2013;

CONSIDERATO, altresì, che con la stessa nota prot. 2356 sopra citata è stato comunicato che la Commissione Europea ha precisato che il caso EU pilot sopra citato potrà essere chiuso soltanto a condizione che l'Italia adotti, entro il 31 ottobre 2013, le modifiche normative annunciate e che si tenga conto delle osservazioni dalla stessa formulate in merito alla citato deliberazione n. 30/2012 sulle modalità per presentare domanda per la certificazione dei sistemi di raccolta elettronica;

RITENUTO di accogliere le richieste di modifica fatte pervenire dalla Commissione Europea;

VISTO il testo, predisposto dall'Ufficio competente e ritenuto di approvarlo;

DETERMINA

1. Di approvare, per i motivi sopra espressi che interamente si richiamano, la procedura per il rilascio della certificazione e della attestazione di conformità dei sistemi di raccolta per via elettronica per l'iniziativa dei cittadini europei, sulla base del testo allegato che costituisce parte integrante della presente determinazione.

2. La presente determinazione sostituisce interamente la deliberazione n. 30 del 29 novembre 2012 del Comitato Direttivo del soppresso DigitPA.

3. L'Ufficio competente curerà gli adempimenti conseguenti alla presente determinazione.

Roma, 23 ottobre 2013

IL DIRETTORE GENERALE IN QUALITA' DI COMMISSARIO STRAORDINARIO

Modalità di presentazione della domanda di certificazione o di attestazione di conformità dei sistemi di raccolta elettronica per le iniziative dei cittadini europei

Allegato alla Determinazione Commissariale n. 168/2013

Modalità di presentazione della domanda di certificazione o di attestazione di conformità dei sistemi di raccolta elettronica per le iniziative dei cittadini europei

1. Definizioni

Ai fini della presente deliberazione si intende per:

a) autorità: l'organismo nazionale designato con DPR 18 ottobre 2012, n. 193 e notificato alla Commissione europea, deputato alla certificazione dei sistemi di raccolta delle dichiarazioni di sostegno;

b) checklist: l'elenco dei controlli da effettuarsi per presentare domanda di certificazione o attestazione di conformità dei sistemi di raccolta, allegati alla presente deliberazione;

c) elenco dei sistemi di raccolta: l'elenco dei sistemi di raccolta delle adesioni per i quali è stata rilasciata la certificazione o l'attestazione di conformità alle normative nazionali e comunitarie vigenti, pubblicato sul sito dell'autorità;

d) firmatari: i cittadini dell'Unione che hanno espresso la propria adesione a una determinata iniziativa dei cittadini di cui al regolamento, compilando l'apposito modulo di sostegno;

e) gestori: le persone giuridiche che hanno ottenuto l'attestazione di conformità del proprio sistema di raccolta allo scopo di renderlo disponibile agli organizzatori interessati;

f) organizzatori: le persone fisiche che hanno formato un comitato dei cittadini promotore di una iniziativa dei cittadini per presentarla alla Commissione europea;

g) rappresentante del comitato: il rappresentante del comitato designato ai sensi dell'art. 3.2 del regolamento;

h) registrazione: la registrazione di una iniziativa legislativa effettuata presso la Commissione europea ai sensi dell'art. 4 del regolamento;

i) regolamento: il Regolamento n. 211/2011 del Parlamento Europeo e del Consiglio del 16 febbraio 2011;

l) regolamento di esecuzione: il Regolamento di esecuzione n. 1179/2011 della Commissione del 17 novembre 2011;

m) sistema di raccolta: sistema informatico costituito da software, hardware, ambiente hosting, processi gestionali e personale, finalizzato alla raccolta delle dichiarazioni di sostegno per via elettronica, previsto dall'art. 6 del regolamento;

n) valutatore: il soggetto deputato alla verifica della conformità del sistema di raccolta con quanto dichiarato dall'organizzatore.

2. Software per la raccolta delle dichiarazioni di sostegno

Gli organizzatori e i gestori hanno la facoltà di utilizzare un proprio software per la raccolta delle dichiarazioni di sostegno online ovvero il software open source reso disponibile dalla Commissione Europea (http://ec.europa.eu/citizens-initiative) ai sensi dell'art. 6 del regolamento, opportunamente integrato nel sistema di raccolta.

L'utilizzo da parte del software fornito dalla Commissione, conformemente all'articolo 6, paragrafo 2, del regolamento, agevola il processo di certificazione riducendo l'ambito della valutazione necessaria per ottenere la certificazione o l'attestazione di conformità del sistema di raccolta.

3. Certificazione del sistema di raccolta

Il regolamento prescrive che il sistema di raccolta per via elettronica delle dichiarazioni di sostegno sia certificato dall'autorità. A tal fine l'organizzatore dell'iniziativa chiede la certificazione del sistema di raccolta per la propria iniziativa con le modalità di cui al punto 4.

Gli organizzatori possono iniziare a raccogliere le dichiarazioni di sostegno mediante il sistema per via elettronica solo dopo aver ottenuto la certificazione del sistema da parte dell'autorità.

4. Domanda di certificazione del sistema di raccolta

Al fine di ottenere la certificazione del sistema di raccolta prevista dal regolamento, l'organizzatore presenta domanda sottoscritta dal rappresentante del comitato.

La documentazione da presentare all'autorità è redatta preferibilmente in forma elettronica, sottoscritta con firma digitale ove prevista la sottoscrizione, e inviata all'indirizzo di posta elettronica certificata dell'autorità pubblicato sul proprio sito istituzionale.

Resta salva, secondo la normativa vigente, la facoltà di redigere i documenti in forma cartacea, che dovranno essere fatti pervenire, congiuntamente alla fotocopia di un documento di riconoscimento in corso di validità del soggetto che sottoscrive la richiesta, all'indirizzo postale dell'autorità.

5. Documentazione da presentare per la richiesta di certificazione

L'organizzatore allega alla domanda di cui al punto 4 le seguenti informazioni, preferibilmente in formato elettronico, sottoscritte dal rappresentante del comitato, con firma digitale se in formato elettronico:

a) titolo della proposta d'iniziativa dei cittadini;

b) dichiarazione circa il luogo in cui sono archiviati i dati ottenuti con le dichiarazioni di sostegno;

c) dichiarazione della conformità del sistema di raccolta oggetto della richiesta di certificazione a quanto prescritto dall'art. 6.4 del regolamento;

d) dichiarazione circa il software utilizzato nel sistema di raccolta;

e) la checklist redatta con le modalità di cui al punto 11;

f) l'eventuale documento previsto al punto 11 contente note e precisazioni concernenti le risposte fornite nella checklist;

g) la documentazione attestante il rispetto dei requisiti previsti dalle norme ISO/IEC 27001 e dal punto 2.2 del regolamento di esecuzione;

h) denominazione, indirizzo mail e numero telefonico del valutatore scelto per la valutazione di conformità al sistema di raccolta con quanto dichiarato dall'organizzatore;

i) indirizzo del sito web (URI) utilizzato per la raccolta delle dichiarazioni di sostegno per l'iniziativa;

l) riferimenti mail, telefonici e postali dell'organizzatore;

m) la dichiarazione del valutatore prevista al punto 11, redatta in lingua italiana.

L'autorità si pronuncia entro un mese decorrente dal momento della presentazione di tutta la documentazione prevista. Eventuali difformità o carenze nella documentazione presentata sono segnalate dall'autorità al richiedente al fine di integrare la documentazione mancante.

Eventuali richieste di integrazione documentale da parte dell'autorità sospendono il termine di cui al periodo precedente fino all'avvenuta consegna del materiale integrativo.

Nel caso in cui quanto necessario per proseguire il processo di certificazione non sia presentato entro sessanta giorni decorrenti dalla richiesta dell'autorità, la richiesta di certificazione è annullata d'ufficio.

6. Validità della certificazione

Il soggetto che richiede e ottiene la certificazione del sistema di raccolta si impegna a mantenere aggiornati i software sottostanti ed i sistemi di protezione.

L'organizzatore si impegna a informare anticipatamente l'autorità di eventuali modifiche ai dati dichiarati nella documentazione, suscettibili di incidere sugli standard tecnici e di sicurezza del sistema di raccolta. L'autorità valuta se, a seguito di tali modifiche, l'organizzatore debba richiedere una nuova certificazione.

7. Attestazione di conformità dei sistemi di raccolta

I gestori che intendono rendere disponibile un sistema di raccolta agli organizzatori devono ottenere l'attestazione di conformità del sistema di raccolta. A tale fine presentano domanda all'autorità ai sensi del punto 8.

8. Domanda di attestazione di conformità dei sistemi di raccolta

I gestori inviano all'indirizzo di posta elettronica certificata dell'autorità domanda di attestazione di conformità del sistema, sottoscritta con firma digitale da un soggetto dotato di potere di firma.

Nella domanda può essere indicato il soggetto responsabile in materia cui si conferisce potere di firma per tutti gli atti e documenti previsti dalla presente deliberazione.

9. Documentazione da presentare per la richiesta di attestazione di conformità

Il gestore allega alla domanda di cui al punto 8 le seguenti informazioni sottoscritte con firma digitale:

a) dichiarazione circa il luogo in cui sono archiviati i dati ottenuti con le dichiarazioni di sostegno;

b) dichiarazione della conformità a quanto prescritto dall'art. 6.4 del regolamento del sistema di raccolta oggetto della richiesta di attestazione di conformità;

c) dichiarazione circa il software utilizzato nel sistema di raccolta;

d) la checklist redatta con le modalità di cui al punto 11;

e) l'eventuale documento previsto al punto 11 contenente note e precisazioni concernenti le risposte fornite nella checklist;

f) la documentazione attestante il rispetto dei requisiti previsti dalle norme ISO/IEC 27001 e dal punto 2.2 del regolamento di esecuzione;

g) copia del certificato di conformità del proprio sistema di gestione per la sicurezza delle informazioni alla norma ISO/IEC 27001, rilasciata da un terzo indipendente a tal fine autorizzato secondo le norme vigenti in materia;

h) riferimenti societari, mail e telefonici del valutatore scelto per la valutazione di conformità al sistema di raccolta con quanto dichiarato dal gestore;

i) riferimenti mail, telefonici e postali del responsabile del sistema di raccolta;

l) copia del certificato attestante la conformità del proprio sistema di qualità alle norme ISO 9000, successive modifiche o a norme equivalenti;

m) la dichiarazione del valutatore prevista al punto 11, redatta in lingua italiana.

L'autorità si pronuncia entro due mesi decorrenti dal momento della presentazione di tutta la documentazione prevista. Eventuali difformità o carenze nella documentazione presentata sono segnalate dall'autorità al richiedente che integra la documentazione mancante.

Eventuali richieste di integrazione documentale da parte dell'autorità sospendono il termine di cui al periodo precedente.

Nel caso in cui quanto necessario per proseguire il processo di certificazione non sia presentato entro trenta giorni decorrenti dalla richiesta dell'autorità, la richiesta di attestazione è annullata d'ufficio.

10. Validità dell'attestazione di conformità

Il gestore che richiede e ottiene l'attestazione di conformità di un sistema di raccolta si impegna a mantenere aggiornati i software sottostanti e i sistemi di protezione.

Al fine di confermare la validità dell'attestazione e i suoi effetti, il gestore invia ogni sei mesi all'autorità una comunicazione in cui dichiara di aver provveduto a quanto stabilito nel periodo precedente e di non aver apportato modifiche al software per la raccolta delle dichiarazioni. L'autorità si riserva la facoltà di verificare la veridicità di dette dichiarazioni.

In assenza della comunicazione semestrale di cui sopra, l'autorità invia un sollecito. Nel caso in cui, decorsi trenta giorni dal sollecito la prevista comunicazione non sia inviata all'autorità, l'attestazione di conformità è revocata d'ufficio. La revoca è resa nota sul sito web dell'autorità.

Il gestore si impegna a comunicare all'autorità entro quindici giorni ogni sopravvenuta variazione a quanto dichiarato nella documentazione presentata.

Fatta eccezione per il software reso disponibile dalla Commissione europea, modifiche al software per la raccolta delle dichiarazioni di sostegno annullano l'attestazione di conformità che dovrà essere nuovamente richiesta. In caso di modifiche non sostanziali, la valutazione di cui al punto 11 potrà limitarsi alle modifiche apportate.

Le attestazioni di conformità devono essere rinnovate ogni due anni. A tale scopo, fermo restando quanto disposto in precedenza, il valutatore di cui al punto 11 verifica e dichiara l'assenza di modifiche al software di raccolta oggetto della precedente valutazione ovvero effettua una nuova e completa valutazione.

Le dichiarazioni del valutatore sono inviate all'autorità che, fatto salvo il diritto di eseguire ulteriori verifiche, estende la validità dell'attestazione di conformità.

11. Valutatori e modalità di valutazione

Ai fini della valutazione, in caso di utilizzo del software reso disponibile dalla Commissione europea, l'interessato compila la checklist di cui all'allegato 1; la checklist di cui all'allegato 2 in caso di utilizzo di altro software. L'interessato, ove necessario, predispone un documento contenente note e precisazioni riguardanti le risposte fornite nella checklist che rende disponibile al valutatore.

La valutazione di conformità del sistema di raccolta con quanto dichiarato nella checklist, è eseguita da un Laboratorio per la Valutazione della Sicurezza informatica (LVS) accreditato secondo lo Schema nazionale per la valutazione e certificazione della sicurezza nel settore della tecnologia dell'informazione dall'Organismo di Certificazione della Sicurezza Informatica (OCSI) o analogo organismo di certificazione che aderisce all'accordo internazionale denominato Common Criteria Recognition Arrangement (CCRA) con il ruolo di Certificate Authorizing Scheme.

Il valutatore dichiara la conformità del sistema di raccolta oggetto di valutazione con quanto dichiarato nella checklist, debitamente compilata e sottoscritta dall'organizzatore, compilando e sottoscrivendo la stessa per quanto di competenza. La dichiarazione deve essere datata, sottoscritta, contenere l'esito della valutazione, contatti mail e telefonici del responsabile della valutazione, gli estremi del sistema di raccolta oggetto di valutazione atti all'individuazione dello stesso, l'hash, calcolato con algoritmo SHA-256, del software per la raccolta delle dichiarazioni di sostegno online.

12. Certificazione dei sistemi di raccolta provvisti di attestazione di conformità

Gli organizzatori possono utilizzare un sistema di raccolta per il quale sia stata emessa una attestazione di conformità in corso di validità. In conformità con il regolamento, è comunque necessario ottenere la certificazione. A tale scopo l'organizzatore consegna la documentazione prevista al punto 5 - escluso quanto indicato alle lettere c), d) e,) f), g), h), m) - e comunica gli estremi del sistema di raccolta, della relativa attestazione di conformità in corso di validità al momento della presentazione della domanda e una dichiarazione del titolare del sistema di

raccolta utilizzato inerente la concessione dell'uso del proprio sistema in favore dell'organizzatore.

I sistemi di raccolta possono condividere alcune risorse conformemente a quanto prescritto al punto 2.8 dell'allegato al regolamento di esecuzione. In questo caso l'autorità, preso atto delle risorse condivise, indica le verifiche che non è necessario ripetere ed eventuali verifiche aggiuntive volte a accertare il rispetto del regolamento di esecuzione.

13. Elenco dei sistemi di raccolta

L'autorità pubblica sul proprio sito internet:

- i sistemi di raccolta in corso di valutazione;
- le certificazioni ed attestazioni di conformità rilasciate;
- il soggetto che ha richiesto la certificazione o attestazione dei sistemi di raccolta;
- gli estremi identificativi dell'iniziativa per i sistemi di raccolta certificati;
- eventuali revoche di certificazioni e attestazioni.

Allegato 1
alla procedura per il rilascio della certificazione e della attestazione di conformità dei sistemi di raccolta per via elettronica per l'iniziativa dei cittadini europei

Checklist per la certificazione ed attestazione di conformità dei sistemi di raccolta nel caso di utilizzo del software fornito dalla Commissione europea

Gli organizzatori, come prescritto al punto 2.1 del regolamento di esecuzione, forniscono la documentazione attestante il rispetto dei requisiti della norma ISO/IEC 27001, senza essere tenuti ad adottarla.

A tal fine essi hanno:

a) effettuato una valutazione completa dei rischi che individua la portata del sistema, evidenzia l'impatto di business in caso di varie violazioni della sicurezza delle informazioni, elenca le minacce cui è esposto il sistema di informazione e le sue vulnerabilità, produce un documento di analisi dei rischi che elenca anche le contromisure per evitarle e i rimedi da adottare se una minaccia si concretizza e infine compila un elenco di miglioramenti, per ordine di priorità;

b) concepito e attuato misure per affrontare i rischi concernenti la protezione dei dati personali e la tutela della vita privata e familiare e definito i provvedimenti da adottare qualora un rischio si verifichi;

c) definito i rischi residui per iscritto;

d) messo in atto i mezzi organizzativi per essere informati sulle nuove minacce e sui miglioramenti in materia di sicurezza.

In base all'analisi dei rischi di cui al punto 2.1, lettera a) del regolamento di esecuzione, gli organizzatori scelgono i controlli di sicurezza da una delle seguenti norme:

1) ISO/IEC 27002; oppure

2) il «Codice di buone pratiche» (Standard of good practices, SoGP) elaborato dall'Information Security Forum;

per affrontare le seguenti questioni:

a) valutazioni dei rischi (si raccomanda di applicare la norma ISO/IEC 27005 o un'altra metodologia specifica ed appropriata di valutazione dei rischi);

b) sicurezza fisica e dell'ambiente;

c) sicurezza delle risorse umane;

d) gestione delle comunicazioni e delle operazioni;

e) misure standard di controllo degli accessi, oltre a quelle stabilite nel regolamento di esecuzione;

f) acquisizione, sviluppo e manutenzione dei sistemi d'informazione;

g) gestione degli incidenti relativi alla sicurezza delle informazioni;

h) misure volte a ridurre e risolvere le violazioni dei sistemi d'informazione, che comporterebbero la distruzione o la perdita accidentale, l'alterazione, l'accesso non autorizzato ai dati personali trattati e la loro diffusione non autorizzata;

i) conformità;

j) sicurezza della rete informatica (si raccomanda di applicare la norma ISO/IEC 27033 o il codice di buone pratiche).

L'applicazione di tali norme può essere limitata alle parti dell'organizzazione che sono pertinenti al sistema di raccolta. Ad esempio, la sicurezza delle risorse umane può essere limitata al personale che ha accesso fisico o in rete al sistema di raccolta elettronica e la sicurezza fisica/dell'ambiente può limitarsi all'edificio o agli edifici che ospitano il sistema.

Minaccia	Contromisura	Source	Implementato	Non applicabile[1]	Rischio accettabile[2]	Verificato dal Valutatore[3]
Autenticazione interrotta e Gestione delle Sessioni	Le password, gli ID di sessione e le altre credenziali sono trasmessi soltanto su connessioni TLS (Transport Layer Security)	*Regolamento di esecuzione - p.2.7.3.g*				
Riferimenti diretti ad oggetti insicuri	Il sistema non ha riferimenti diretti a oggetti non sicuri	*Regolamento di esecuzione - p.2.7.4*				
Riferimenti diretti ad oggetti insicuri	Per i riferimenti diretti ad una risorsa soggetta a restrizioni di accesso, l'applicazione verifica che l'utente sia autorizzato ad accedere alla risorsa richiesta	*Regolamento di esecuzione - p.2.7.4.a*				

[1] In caso di non applicabilità del requisito nella cella si deve far riferimento al paragrafo del documento "Note" in cui è descritta la motivazione.
[2] In caso di rischio ritenuto accettabile nella cella si deve far riferimento al paragrafo del documento "Note" in cui è descritta la motivazione.
[3] Il valutatore verifica e conferma la correttezza della risposta, ovvero introduce un riferimento contenuto nella dichiarazione di cui al punto 11 della Deliberazione, in cui motiva la non conformità.

Minaccia	Contromisura	Source	Implementato	Non applicabile[1]	Rischio accettabile[2]	Verificato dal Valutatore[3]
Riferimenti diretti ad oggetti insicuri	Se il riferimento è di tipo indiretto, il mapping al riferimento diretto è limitato ai valori autorizzati per l'utente corrente	*Regolamento di esecuzione - p.2.7.4.b*				
Sfruttamento Transport Layer insufficiente	Per accedere alle risorse riservate il sistema richiede la versione più recente del protocollo HTTPS (Secure HyperText Transfer Protocol) utilizzando certificati validi, non scaduti, non revocati e che corrispondano a tutti i nomi di dominio utilizzati dal sito	*Regolamento di esecuzione - p.2.7.9.a*				
Sfruttamento Transport Layer insufficiente	Il flag «secure» deve essere impostato per tutti i cookie riservati	*Regolamento di esecuzione - p.2.7.9.b*				
Sfruttamento Transport Layer insufficiente	La connessione TLS è configurata per supportare unicamente algoritmi di cifratura conformi alle migliori pratiche; gli utenti sono consapevoli di dover attivare l'opzione TLS nel loro browser	*Regolamento di esecuzione - p.2.7.9.c*				

Minaccia	Contromisura	Source	Implementato	Non applicabile[1]	Rischio accettabile[2]	Verificato dal Valutatore[3]
Network Eavesdropping	La sessione di accesso dell'amministratore all'interfaccia di gestione del sistema di raccolta ha un breve tempo di validità (massimo 15 minuti).	*Regolamento di esecuzione - p.2.19.3*				
Accesso non autorizzato	Esistono registri di tutte le attività del sistema. Il sistema garantisce che vi siano registri di controllo, che tengono traccia delle eccezioni e degli altri eventi in materia di sicurezza elencati qui di seguito, e che siano mantenuti fino a quando i dati sono distrutti a norma dell'articolo 12, paragrafo 3 o paragrafo 5, del Regolamento (UE) n. 211/2011. I registri sono adeguatamente salvaguardati, ad esempio, mediante l'archiviazione su supporti cifrati. Gli organizzatori/amministratori controllano regolarmente i registri per verificare se vi sono attività sospette. I registri contengono almeno: a) data e ora di connessione e disconnessione degli organizzatori/amministratori; b) copie di sicurezza effettuate; c) tutte le modifiche e gli aggiornamenti relativi all'amministratore	*Regolamento di esecuzione - p.2.16*				

Minaccia	Contromisura	Source	Implementato	Non applicabile[1]	Rischio accettabile[2]	Verificato dal Valutatore[3]
	della banca dati.					

Minaccia	Contromisura	Source	Implementato	Non applicabile[1]	Rischio accettabile[2]	Verificato dal Valutatore[3]
Accesso non autorizzato	Esiste una configurazione di sicurezza adeguata che rispetta i requisiti minimi seguenti: a) tutti i componenti software sono aggiornati, compresi il sistema operativo, il server di rete/dell'applicazione, il sistema di gestione di basi dati (Data Base Management System — DBMS), le applicazioni, e tutte le librerie di codice; b) tutti gli elementi non necessari del sistema operativo e del server di rete/dell'applicazione sono disattivati, rimossi o non installati; c) le password di default dell'account sono cambiate o disattivate; d) la gestione degli errori è attivata per prevenire la visualizzazione dello stack trace e di altri messaggi di errore che potrebbero far trapelare informazioni utili; e) le impostazioni di sicurezza dei framework di sviluppo e delle librerie sono configurate in conformità con le migliori pratiche, quali ad esempio le linee guida dell'OWASP.	*Regolamento di esecuzione - p.2.7.6*				

Minaccia	Contromisura	Source	Implementato	Non applicabile[1]	Rischio accettabile[2]	Verificato dal Valutatore[3]
Accesso non autorizzato	Il sistema di gestione di basi dati (DBMS) utilizzato è costantemente aggiornato con nuove patch contro le vulnerabilità scoperte di recente.	*Regolamento di esecuzione - p.2.15*				
Accesso non autorizzato	Sicurezza fisica Indipendentemente dal tipo di hosting utilizzato, l'elaboratore che ospita l'applicazione è adeguatamente protetto, e dispone di: a) controllo degli accessi all'area di hosting e registri di controllo; b) protezione fisica della copia di sicurezza dei dati contro il furto o la collocazione errata accidentale; c) installazione del server che ospita l'applicazione in un rack sicuro.	*Regolamento di esecuzione - p.2.17*				
Accesso non autorizzato	Il sistema è ospitato su un server connesso a Internet installato in una zona demilitarizzata e protetto da un firewall.	*Regolamento di esecuzione - p.2.18.1*				

Minaccia	Contromisura	Source	Implementato	Non applicabile[1]	Rischio accettabile[2]	Verificato dal Valutatore[3]
Accesso non autorizzato	Quando vengono resi pubblici aggiornamenti e patch pertinenti al prodotto firewall, tali aggiornamenti o patch sono tempestivamente installati.	*Regolamento di esecuzione - p.2.18.2*				
Accesso non autorizzato	Tutto il traffico in entrata e in uscita dal server (destinato al sistema di raccolta) viene esaminato secondo le regole del firewall e registrato. Le regole del firewall respingono tutto il traffico che non è necessario per l'utilizzo e la gestione in sicurezza del sistema.	*Regolamento di esecuzione - p.2.18.3*				
Accesso non autorizzato	Il sistema di raccolta deve essere ospitato su un segmento della rete per la produzione adeguatamente protetto che è separato dai segmenti utilizzati per ospitare sistemi non diretti alla produzione, quali ambienti di sviluppo o sperimentazione.	*Regolamento di esecuzione - p.2.18.4*				

Minaccia	Contromisura	Source	Implementato	Non applicabile[1]	Rischio accettabile[2]	Verificato dal Valutatore[3]
Accesso non autorizzato	Sono implementate misure di sicurezza delle rete locale (LAN), quali: a) liste di controllo di accessi Layer 2 (L2); sicurezza delle porte dello switch; b) tutte le porte dello switch non in uso sono disabilitate; c) la zona demilitarizzata è su un'apposita rete locale virtuale (VLAN)/LAN; d) nelle porte non necessarie non è abilitato il trunk di L2.	*Regolamento di esecuzione - p.2.18.5*				
Accesso non autorizzato	Quando sono resi pubblici aggiornamenti e patch del sistema operativo, dei tempi di esecuzione dell'applicazione, delle applicazioni in funzione sui server o dei programmi anti-malware, tali aggiornamenti o patch sono tempestivamente installati.	*Regolamento di esecuzione - p.2.19.4*				

Minaccia	Contromisura	Source	Implementato	Non applicabile[1]	Rischio accettabile[2]	Verificato dal Valutatore[3]
Accesso non autorizzato	Ai fini della sicurezza da utente a utente, gli organizzatori adottano le misure necessarie per proteggere l'applicazione/dispositivo client che utilizzano per gestire il sistema di raccolta e per accedervi	*Regolamento di esecuzione - p.2.20*				
Accesso non autorizzato	Gli utenti eseguono compiti non attinenti alla manutenzione (quale l'automazione d'ufficio) con i privilegi minimi necessari.	*Regolamento di esecuzione - p.2.20.1*				
Accesso non autorizzato	Quando vengono resi pubblici aggiornamenti e patch del sistema operativo, delle applicazioni installate o del programma anti-malware, tali aggiornamenti o patch sono tempestivamente installati.	*Regolamento di esecuzione - p.2.20.2*				
Accesso non autorizzato	È impostata una corretta configurazione di sicurezza, compresi gli elementi elencati al punto 2.7.6.	*Regolamento di esecuzione - p.2.19.1*				

Minaccia	Contromisura	Source	Implementato	Non applicabile[1]	Rischio accettabile[2]	Verificato dal Valutatore[3]
Accesso non autorizzato	Il rischio che una persona si identifichi nel sistema utilizzando lo strumento «pass-the-hash» è attenuato.	*Regolamento di esecuzione - p.2.19.5*				

IMPLEMENTAZIONE DELL'ARTICOLO 6(4)(c) DEL REGOLAMENTO (EU) No 211/2011 ***(Regolamento di esecuzione – Point 3.4)***	**STATUS**		
	Implementato	**Non implementato**	**Verificato dal valutatore**
La trasmissione elettronica dei dati esportati agli Stati membri è protetta da intercettazioni mediante cifratura da punto a punto.			

Allegato 2
alla procedura per il rilascio della certificazione e della attestazione di conformità dei sistemi di raccolta per via elettronica per l'iniziativa dei cittadini europei

Checklist per la certificazione ed attestazione di conformità dei sistemi di raccolta nel caso di utilizzo di software non fornito dalla Commissione europea

Gli organizzatori, come prescritto al punto 2.1 del regolamento di esecuzione, forniscono la documentazione attestante il rispetto dei requisiti della norma ISO/IEC 27001, senza essere tenuti ad adottarla.

A tal fine essi hanno:

a) effettuato una valutazione completa dei rischi che individua la portata del sistema, evidenzia l'impatto di business in caso di varie violazioni della sicurezza delle informazioni, elenca le minacce cui è esposto il sistema di informazione e le sue vulnerabilità, produce un documento di analisi dei rischi che elenca anche le contromisure per evitarle e i rimedi da adottare se una minaccia si concretizza e infine compila un elenco di miglioramenti, per ordine di priorità;

b) concepito e attuato misure per affrontare i rischi concernenti la protezione dei dati personali e la tutela della vita privata e familiare e definito i provvedimenti da adottare qualora un rischio si verifichi;

c) definito i rischi residui per iscritto;

d) messo in atto i mezzi organizzativi per essere informati sulle nuove minacce e sui miglioramenti in materia di sicurezza.

In base all'analisi dei rischi di cui al punto 2.1, lettera a) del regolamento di esecuzione, gli organizzatori scelgono i controlli di sicurezza da una delle seguenti norme:

1) ISO/IEC 27002; oppure

2) il «Codice di buone pratiche» (Standard of good practices, SoGP) elaborato dall'Information Security Forum;

per affrontare le seguenti questioni:

a) valutazioni dei rischi (si raccomanda di applicare la norma ISO/IEC 27005 o un'altra metodologia specifica ed appropriata di valutazione dei rischi);

b) sicurezza fisica e dell'ambiente;

c) sicurezza delle risorse umane;

d) gestione delle comunicazioni e delle operazioni;

e) misure standard di controllo degli accessi, oltre a quelle stabilite nel regolamento di esecuzione;

f) acquisizione, sviluppo e manutenzione dei sistemi d'informazione;

g) gestione degli incidenti relativi alla sicurezza delle informazioni;

h) misure volte a ridurre e risolvere le violazioni dei sistemi d'informazione, che comporterebbero la distruzione o la perdita accidentale, l'alterazione, l'accesso non autorizzato ai dati personali trattati e la loro diffusione non autorizzata;

i) conformità;

j) sicurezza della rete informatica (si raccomanda di applicare la norma ISO/IEC 27033 o il codice di buone pratiche).

L'applicazione di tali norme può essere limitata alle parti dell'organizzazione che sono pertinenti al sistema di raccolta. Ad esempio, la sicurezza delle risorse umane può essere limitata al personale che ha accesso fisico o in rete al sistema di raccolta e la sicurezza fisica/dell'ambiente può limitarsi all'edificio o agli edifici che ospitano il sistema.

REQUISITI FUNZIONALI	**STATUS**		
	Implementato	**Non implementato**	**Verificato dal valutatore**[4]
Il sistema di raccolta è costituito da un'istanza applicativa basata su web creata allo scopo di raccogliere le dichiarazioni di sostegno per un'unica iniziativa dei cittadini. *(Regolamento di esecuzione – punto 2.3)*			

[4] Il valutatore verifica e conferma la correttezza della risposta, ovvero introduce un riferimento contenuto nella dichiarazione di cui al punto 11 della Deliberazione, in cui motiva la non conformità.

REQUISITI FUNZIONALI	STATUS		
	Implementato	Non implementato	Verificato dal valutatore[4]
Se la gestione del sistema richiede diversi ruoli, i differenti livelli di controllo degli accessi sono stabiliti in base al principio del privilegio minimo. *(Regolamento di esecuzione – punto 2.4)*			
Le funzionalità accessibili al pubblico sono nettamente distinte da quelle a scopo amministrativo. La lettura delle informazioni disponibili nell'area pubblica del sistema, comprese le informazioni sull'iniziativa e il modulo elettronico per la dichiarazione di sostegno, non è ostacolata da un controllo degli accessi. È possibile firmare a sostegno di un'iniziativa solo attraverso quest'area pubblica. *(Regolamento di esecuzione – punto 2.5)*			

REQUISITI FUNZIONALI	STATUS		
	Implementato	Non implementato	Verificato dal valutatore[4]
Il sistema rileva e impedisce la duplice trasmissione delle dichiarazioni di sostegno. *(Regolamento di esecuzione – punto 2.6)*			

Minaccia	Contromisura	Riferimento	Implementato	Non applicabile[5]	Rischio accettabile[6]	Verificato dal Valutatore[7]
Injection	Il sistema è protetto contro attacchi da iniezione (injection flaws), ad esempio attraverso interrogazioni SQL (Structured Query Language), LDAP (Lightweight Directory Access Protocol), in linguaggio XML Path (XPath), i comandi del sistema operativo o gli argomenti del programma.	*Regolamento di esecuzione – punto 2.7.1*				
Injection	Tutti i dati di input forniti dagli utenti sono validati;	*Regolamento di esecuzione– punto 2.7.1.a*				
Injection	La convalida è effettuata almeno applicando la logica lato server	*Regolamento di esecuzione – punto 2.7.1.b*				

[5] In caso di non applicabilità del requisito nella cella si deve far riferimento al paragrafo del documento "Note" in cui è descritta la motivazione.
[6] In caso di rischio ritenuto accettabile nella cella si deve far riferimento al paragrafo del documento "Note" in cui è descritta la motivazione.
[7] Il valutatore verifica e conferma la correttezza della risposta, ovvero introduce un riferimento contenuto nella dichiarazione di cui al punto 11 della Deliberazione, in cui motiva la non conformità.

Minaccia	Contromisura	Riferimento	Implementato	Non applicabile[5]	Rischio accettabile[6]	Verificato dal Valutatore[7]
Injection	Qualsiasi utilizzo di interpreti si basa sulla separazione netta dei dati non affidabili dai comandi o dalle interrogazioni. Per richieste SQL, questo comporta l'uso di variabili bind in tutte le istruzioni preparate e le procedure archiviate, evitando le query di tipo dinamico.	Regolamento di esecuzione – *punto 2.7.1.c*				
Cross-Site Scripting (XSS)	Tutti i dati di input forniti dall'utente e rinviati al browser sono controllati sotto il profilo della sicurezza (attraverso una validazione degli input)	*Regolamento di esecuzione – punto 2.7.2.a*				
Cross-Site Scripting (XSS)	Tutti i dati di input forniti dall'utente sono sottoposti ad una adeguata sequenza di escape prima di essere ripresi nella pagina finale	*Regolamento di esecuzione – punto 2.7.2.b*				
Cross-Site Scripting (XSS)	Un'adeguata codifica di output garantisce che tali dati di input siano sempre considerati come testo nel browser. Non sono utilizzati contenuti attivi	*Regolamento di esecuzione – punto 2.7.2.c*				

Minaccia	Contromisura	Riferimento	Implementato	Non applicabile[5]	Rischio accettabile[6]	Verificato dal Valutatore[7]
Autenticazione interrotta e Gestione delle Sessioni	Il sistema ha una rigorosa gestione delle autenticazioni e delle sessioni	*Regolamento di esecuzione – punto 2.7.3*				
Autenticazione interrotta e Gestione delle Sessioni	Le credenziali sono sempre protette, al momento dell'archiviazione, con tecniche di hashing o crittografia; il rischio che una persona si identifichi utilizzando lo strumento «pass-the-hash» è attenuato	*Regolamento di esecuzione – punto 2.7.3.a*				
Autenticazione interrotta e Gestione delle Sessioni	Le credenziali non possono essere indovinate o sovrascritte sfruttando carenze nelle funzioni di gestione degli account [ad esempio creazione dell'account, modifica e recupero della password, deboli identificativi di sessione (ID)]	*Regolamento di esecuzione – punto 2.7.3.b*				

Minaccia	Contromisura	Riferimento	Implementato	Non applicabile[5]	Rischio accettabile[6]	Verificato dal Valutatore[7]
Autenticazione interrotta e Gestione delle Sessioni	L'id di sessione e i dati relativi alla sessione non appaiono nell'URL	*Regolamento di esecuzione – punto 2.7.3.c*				
Autenticazione interrotta e Gestione delle Sessioni	L'id di sessione non è vulnerabile ad attacchi di fissazione di sessione	*Regolamento di esecuzione – punto 2.7.3.d*				
Autenticazione interrotta e Gestione delle Sessioni	L'id di sessione ha un tempo di validità (ID timeout), che garantisce la disconnessione degli utenti	*Regolamento di esecuzione – punto 2.7.3.e*				

Minaccia	Contromisura	Riferimento	Implementato	Non applicabile[5]	Rischio accettabile[6]	Verificato dal Valutatore[7]
Autenticazione interrotta e Gestione delle Sessioni	Gli ID di sessione non sono rinnovati dopo un'autenticazione riuscita	*Regolamento di esecuzione – punto 2.7.3.f*				
Utilizzo dei dati crittografici memorizzati non sicuro	I dati personali in formato elettronico sono cifrati quando sono archiviati o trasmessi alle autorità competenti degli Stati membri ai sensi dell'articolo 8, paragrafo 1, del Regolamento (UE) n. 211/2011; le chiavi sono gestite e salvate separatamente	*Regolamento di esecuzione – punto 2.7.7.a*				
Utilizzo dei dati crittografici memorizzati non sicuro	Sono utilizzati algoritmi standard e chiavi di cifratura robusti, in linea con gli standard internazionali. Esiste una gestione delle chiavi	*Regolamento di esecuzione – punto 2.7.7.b*				

Minaccia	Contromisura	Riferimento	Implementato	Non applicabile[5]	Rischio accettabile[6]	Verificato dal Valutatore[7]
Utilizzo dei dati crittografici memorizzati non sicuro	Le password sono protette da algoritmi standard di hash robusti che utilizzano adeguati parametri salt	*Regolamento di esecuzione – punto 2.7.7.c*				
Utilizzo dei dati crittografici memorizzati non sicuro	Tutte le chiavi e le password sono protette da accessi non autorizzati.	*Regolamento di esecuzione – punto 2.7.7.d*				
Utilizzo dei dati crittografici memorizzati non sicuro	Le credenziali amministrative, i dati personali raccolti dai firmatari e la loro copia di sicurezza (backup) sono protetti mediante algoritmi robusti in linea con il punto 2.7.7, lettera b). Tuttavia, l'indicazione dello Stato membro in cui la dichiarazione di sostegno sarà contata, la data di presentazione della dichiarazione di sostegno e la lingua nella quale il firmatario ha compilato il modulo di dichiarazione di sostegno possono essere archiviati nel sistema senza essere cifrati.	*Regolamento di esecuzione – punto 2.11*				

Minaccia	Contromisura	Riferimento	Implementato	Non applicabile[5]	Rischio accettabile[6]	Verificato dal Valutatore[7]
Utilizzo dei dati crittografici memorizzati non sicuro	I dati personali dei firmatari, comprese le copie di sicurezza, sono disponibili nel sistema esclusivamente in forma cifrata. Ai fini della verifica o della certificazione dei dati da parte delle autorità nazionali a norma dell'articolo 8 del Regolamento (UE) n. 211/2011, gli organizzatori possono esportare i dati cifrati conformemente al punto 2.7.7, lettera a).	*Regolamento di esecuzione – punto 2.13*				
Restrict URL: accesso fallito	Se per gestire le autenticazioni e le autorizzazioni per l'accesso alle pagine sono utilizzati meccanismi di sicurezza esterni, questi devono essere correttamente configurati per tutte le pagine	*Regolamento di esecuzione – punto 2.7.8.a*				
Restrict URL: accesso fallito	Se è utilizzata una protezione a livello di codice, la protezione è applicata per tutte le pagine richieste.	*Regolamento di esecuzione – punto 2.7.8.b*				
Attacco Brute Force	La sezione amministrativa del sistema è protetta. Se è protetta da un'autenticazione a fattore unico, la password deve essere composta da almeno 10 caratteri, fra cui almeno una lettera, un numero e un	*Regolamento di esecuzione – punto 2.7.3.h*				

Minaccia	Contromisura	Riferimento	Implementato	Non applicabile[5]	Rischio accettabile[6]	Verificato dal Valutatore[7]
	carattere speciale. In alternativa può essere utilizzata l'autenticazione a doppio fattore. Qualora sia utilizzata unicamente l'autenticazione a fattore unico, essa comprende un meccanismo di verifica in due fasi per l'accesso alla sezione amministrativa del sistema via internet, in cui al fattore unico si aggiunga un altro mezzo di autenticazione, come una frase password/codice validi per un solo utilizzo inviati per SMS o una stringa di caratteri casuali criptata con algoritmo asimmetrico da decriptare utilizzando la chiave privata degli organizzatori/amministratori, sconosciuta al sistema.					
Accesso non autorizzato	I firmatari hanno accesso ai dati forniti solamente durante la sessione in cui compilano il modulo di dichiarazione di sostegno: una volta inviato il modulo, la sessione è conclusa e i dati trasmessi non sono più accessibili.	*Regolamento di esecuzione – punto 2.12*				
Accesso non autorizzato	Sebbene i sistemi di raccolta utilizzati per varie iniziative dei cittadini condividano l'hardware e le risorse del sistema operativo, essi non condividono alcun dato, comprese le credenziali di accesso/cifratura.	*Regolamento di esecuzione –*				

Minaccia	Contromisura	Riferimento	Implementato	Non applicabile[5]	Rischio accettabile[6]	Verificato dal Valutatore[7]
	Lo stesso vale per la valutazione dei rischi e le contromisure attuate.	*punto 2.8*				

Accesso non autorizzato	I dati forniti dai firmatari sono accessibili soltanto all'amministratore/organizzatore della banca dati.	*Regolamento di esecuzione - punto 2.10*				
Accesso non autorizzato	Le applicazioni funzionano con il minimo dei privilegi necessari.	*Regolamento di esecuzione – punto 2.19.2*				
Applicazione fallita	La persistenza dei dati inseriti nel modulo di dichiarazione di sostegno è da considerare indivisibile, cioè una volta che l'utente ha inserito tutte le informazioni richieste nel modulo di dichiarazione di sostegno e convalidato la sua decisione di sostenere l'iniziativa, il sistema invia tutti i dati del modulo alla banca dati, oppure, in caso di errore, non salva nessun dato. Il sistema informa l'utente se la sua richiesta è andata o meno a buon fine.	*Regolamento di esecuzione – punto 2.14*				
Autenticazione interrotta e Gestione delle Sessioni	Le password, gli ID di sessione e le altre credenziali sono trasmessi soltanto su connessioni TLS (Transport Layer Security)	*Regolamento di esecuzione – punto 2.7.3.g*				
Utilizzo Direct Object References non sicuro	Il sistema non ha riferimenti diretti a oggetti non sicuri.	*Regolamento di esecuzione – punto 2.7.4*				

Utilizzo Direct Object References non sicuro	Per i riferimenti diretti ad una risorsa soggetta a restrizioni di accesso, l'applicazione verifica che l'utente sia autorizzato ad accedere alla risorsa richiesta	*Regolamento di esecuzione – punto 2.7.4.a*				
Utilizzo Direct Object References non sicuro	Se il riferimento è di tipo indiretto, il mapping al riferimento diretto è limitato ai valori autorizzati per l'utente corrente.	*Regolamento di esecuzione – punto 2.7.4.b*				
Utilizzo Transport Layer insufficiente	Per accedere alle risorse riservate il sistema richiede la versione più recente del protocollo HTTPS (Secure HyperText Transfer Protocol) utilizzando certificati validi, non scaduti, non revocati e che corrispondano a tutti i nomi di dominio utilizzati dal sito	*Regolamento di esecuzione – punto 2.7.9.a*				
Utilizzo Transport Layer insufficiente	Il flag «secure» deve essere impostato per tutti i cookie riservati	*Regolamento di esecuzione – punto 2.7.9.b*				
Utilizzo Transport Layer insufficiente	La connessione TLS è configurata per supportare unicamente algoritmi di cifratura conformi alle migliori pratiche; gli utenti sono consapevoli di dover attivare l'opzione TLS nel loro browser.	*Regolamento di esecuzione – punto 2.7.9.c*				
Network Eavesdropping	La sessione di accesso dell'amministratore all'interfaccia di gestione del sistema di raccolta ha un breve tempo di validità (massimo 15 minuti).	*Regolamento di esecuzione – punto 2.19.3*				

Accesso non autorizzato	Esistono registri di tutte le attività del sistema. Il sistema garantisce che vi siano registri di controllo, che tengono traccia delle eccezioni e degli altri eventi in materia di sicurezza elencati qui di seguito, e che siano mantenuti fino a quando i dati sono distrutti a norma dell'articolo 12, paragrafo 3 o paragrafo 5, del Regolamento (UE) n. 211/2011. I registri sono adeguatamente salvaguardati, ad esempio, mediante l'archiviazione su supporti cifrati. Gli organizzatori/amministratori controllano regolarmente i registri per verificare se vi sono attività sospette. I registri contengono almeno: a) data e ora di connessione e disconnessione degli organizzatori/amministratori; b) copie di sicurezza effettuate; c) tutte le modifiche e gli aggiornamenti relativi all'amministratore della banca dati.	*Regolamento di esecuzione – punto 2.16*				
Accesso non autorizzato	Esiste una configurazione di sicurezza adeguata che rispetta i requisiti minimi seguenti: a) tutti i componenti software sono aggiornati, compresi il sistema operativo, il server di rete/dell'applicazione, il sistema di gestione di basi dati (Data Base Management System — DBMS), le applicazioni, e tutte le librerie di codice;	*Regolamento di esecuzione – punto 2.7.6*				

	b) tutti gli elementi non necessari del sistema operativo e del server di rete/dell'applicazione sono disattivati, rimossi o non installati; c) le password di default dell'account sono cambiate o disattivate; d) la gestione degli errori è attivata per prevenire la visualizzazione dello stack trace e di altri messaggi di errore che potrebbero far trapelare informazioni utili; e) le impostazioni di sicurezza dei framework di sviluppo e delle librerie sono configurate in conformità con le migliori pratiche, quali ad esempio le linee guida dell'OWASP.					
Accesso non autorizzato	Il sistema di gestione di basi dati (DBMS) utilizzato è costantemente aggiornato con nuove patch contro le vulnerabilità scoperte di recente.	*Regolamento di esecuzione – punto 2.15*				
Accesso non autorizzato	*Sicurezza fisica* Indipendentemente dal tipo di hosting utilizzato, l'elaboratore che ospita l'applicazione è adeguatamente protetto, e dispone di: a) controllo degli accessi all'area di hosting e registri di controllo; b) protezione fisica della copia di sicurezza dei dati contro il furto o la collocazione errata accidentale; c) installazione del server che ospita l'applicazione in un rack sicuro.	*Regolamento di esecuzione – punto 2.17*				

Accesso non autorizzato	Il sistema è ospitato su un server connesso a Internet installato in una zona demilitarizzata e protetto da un firewall.	*Regolamento di esecuzione – punto 2.18.1*				
Accesso non autorizzato	Quando vengono resi pubblici aggiornamenti e patch pertinenti al prodotto firewall, tali aggiornamenti o patch sono tempestivamente installati.	*Regolamento di esecuzione – punto 2.18.2*				
Accesso non autorizzato	Tutto il traffico in entrata e in uscita dal server (destinato al sistema di raccolta) viene esaminato secondo le regole del firewall e registrato. Le regole del firewall respingono tutto il traffico che non è necessario per l'utilizzo e la gestione in sicurezza del sistema.	*Regolamento di esecuzione – punto 2.18.3*				
Accesso non autorizzato	Il sistema di raccolta deve essere ospitato su un segmento della rete per la produzione adeguatamente protetto che è separato dai segmenti utilizzati per ospitare sistemi non diretti alla produzione, quali ambienti di sviluppo o sperimentazione.	*Regolamento di esecuzione – punto 2.18.4*				
Accesso non autorizzato	Sono implementate misure di sicurezza delle rete locale (LAN), quali: a) liste di controllo di accessi Layer 2 (L2); sicurezza delle porte dello switch; b) tutte le porte dello switch non in uso sono disabilitate; c) la zona demilitarizzata è su un'apposita rete locale virtuale (VLAN)/LAN;	*Regolamento di esecuzione – punto 2.18.5*				

	d) nelle porte non necessarie non è abilitato il trunk di L2.					
Accesso non autorizzato	Quando sono resi pubblici aggiornamenti e patch del sistema operativo, dei tempi di esecuzione dell'applicazione, delle applicazioni in funzione sui server o dei programmi anti-malware, tali aggiornamenti o patch sono tempestivamente installati.	*Regolamento di esecuzione – punto 2.19.4*				
Accesso non autorizzato	Ai fini della sicurezza da utente a utente, gli organizzatori adottano le misure necessarie per proteggere l'applicazione/dispositivo client che utilizzano per gestire il sistema di raccolta e per accedervi	*Regolamento di esecuzione – punto 2.20*				
Accesso non autorizzato	Gli utenti eseguono compiti non attinenti alla manutenzione (quale l'automazione d'ufficio) con i privilegi minimi necessari.	*Regolamento di esecuzione – punto 2.20.1*				
Accesso non autorizzato	Quando vengono resi pubblici aggiornamenti e patch del sistema operativo, delle applicazioni installate o del programma anti-malware, tali aggiornamenti o patch sono tempestivamente installati.	*Regolamento di esecuzione – punto 2.20.2*				
Accesso non autorizzato	Il sistema protegge contro gli attacchi di tipo CSRF (Cross Site Request Forgery).	*Regolamento di esecuzione – punto 2.7.5*				

Accesso non autorizzato	Il sistema protegge contro reindirizzamenti automatici non validati.	*Regolamento di esecuzione – punto 2.7.10*				
Accesso non autorizzato	Il rischio che una persona si identifichi nella base dati utilizzando lo strumento «pass-the-hash» è attenuato.	*Regolamento di esecuzione – punto 2.9*				
Accesso non autorizzato	È impostata una corretta configurazione di sicurezza, compresi gli elementi elencati al punto 2.7.6.	*Regolamento di esecuzione – punto 2.19.1*				
Accesso non autorizzato	Il rischio che una persona si identifichi nel sistema utilizzando lo strumento «pass-the-hash» è attenuato.	*Regolamento di esecuzione – punto 2.19.5*				

IMPLEMENTAZIONE DELL'ARTICOLO 6(4)(c) DEL REGOLAMENTO (EU) No 211/2011	STATUS		
	Implementato	Non implementato	Verificato dal valutatore
Il sistema prevede la possibilità di estrarre per ogni singolo Stato membro un rapporto contenente l'iniziativa e l'elenco dei dati personali dei firmatari soggetti a verifica da parte dell'autorità competente di detto Stato membro. (*Regolamento di esecuzione – punto 3.1*)			

IMPLEMENTAZIONE DELL'ARTICOLO 6(4)(c) DEL REGOLAMENTO (EU) No 211/2011	STATUS		
	Implementato	Non implementato	Verificato dal valutatore
L'esportazione delle dichiarazioni di sostegno dei firmatari è possibile nel formato di cui all'allegato III del Regolamento (UE) n. 211/2011. Il sistema può inoltre prevedere la possibilità di esportare le dichiarazioni di sostegno in formato interoperabile, come il formato XML. (*Regolamento di esecuzione – punto 3.2*)			
Le dichiarazioni di sostegno esportate verso lo Stato membro interessato sono contrassegnate dalla dicitura «*diffusione limitata*», e classificate come «*dati personali*». (*Regolamento di esecuzione – punto 3.3*)			

IMPLEMENTAZIONE DELL'ARTICOLO 6(4)(a) DEL REGOLAMENTO (EU) No 211/2011	STATUS		
	Implementato	Non implementato	Verificato dal valutatore
Per evitare la trasmissione automatizzata delle dichiarazioni di sostegno attraverso il sistema, il firmatario è sottoposto a un adeguato processo di verifica in linea con la prassi attuale prima di inviare la propria dichiarazione. Un possibile metodo di verifica è l'impiego di un captcha robusto. (*Regolamento di esecuzione – punto 1*)			