II

(Atti non legislativi)

REGOLAMENTI

REGOLAMENTO DI ESECUZIONE (UE) N. 1179/2011 DELLA COMMISSIONE

del 17 novembre 2011

che fissa le specifiche tecniche per i sistemi di raccolta elettronica a norma del regolamento (UE) n. 211/2011 del Parlamento europeo e del Consiglio riguardante l'iniziativa dei cittadini

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) n. 211/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, riguardante l'iniziativa dei cittadini [1], in particolare l'articolo 6, paragrafo 5,

sentito il Garante europeo della protezione dei dati,

considerando quanto segue:

(1) Il regolamento (UE) n. 211/2011 prevede che se le dichiarazioni di sostegno sono raccolte per via elettronica, il sistema utilizzato a tal fine deve soddisfare determinati requisiti tecnici e di sicurezza e deve essere certificato dall'autorità competente dello Stato membro interessato.

(2) Un sistema di raccolta per via elettronica ai sensi del regolamento (UE) n. 211/2011 è un sistema informatico, costituito di software, hardware, ambiente hosting, processi gestionali e personale, finalizzato alla raccolta delle dichiarazioni di sostegno per via elettronica.

(3) Il regolamento (UE) n. 211/2011 definisce i requisiti che i sistemi di raccolta per via elettronica devono rispettare per ricevere la certificazione e prevede che la Commissione adotti specifiche tecniche per l'attuazione di tali requisiti.

(4) L'edizione 2010 del progetto Top 10 dell'OWASP (Open Web Application Security Project) fornisce una panoramica dei rischi maggiormente critici per la sicurezza delle applicazioni web, nonché degli strumenti per prevenirli; le specifiche tecniche si basano quindi sulle conclusioni di questo progetto.

(5) L'attuazione delle specifiche tecniche da parte degli organizzatori garantisce la certificazione dei sistemi di raccolta per via elettronica da parte delle autorità degli Stati membri e contribuisce ad assicurare l'attuazione delle opportune misure tecniche e organizzative necessarie per rispettare gli obblighi imposti dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio [2] sulla sicurezza delle operazioni di trattamento, sia al momento della progettazione del sistema di trattamento che durante il trattamento stesso, al fine di mantenere la sicurezza, impedendo pertanto qualsiasi trattamento non autorizzato, e proteggere i dati personali da distruzione accidentale o dolosa, da perdita e alterazione accidentali o da diffusione o accesso non autorizzati.

(6) L'utilizzo da parte degli organizzatori del software fornito dalla Commissione, conformemente all'articolo 6, paragrafo 2, del regolamento (UE) n. 211/2011, agevola il processo di certificazione.

(7) Nel corso della raccolta delle dichiarazioni di sostegno per via elettronica gli organizzatori di un'iniziativa dei cittadini, in qualità di responsabili del trattamento dei dati, attuano le specifiche tecniche di cui al presente regolamento al fine di garantire la protezione dei dati personali trattati. Qualora il trattamento sia effettuato da un responsabile del trattamento, gli organizzatori garantiscono che l'incaricato agisce soltanto su loro istruzioni e attua le specifiche tecniche stabilite nel presente regolamento.

(8) Il presente regolamento rispetta i diritti fondamentali e ottempera ai principi enunciati nella Carta dei diritti fondamentali dell'Unione europea, in particolare all'articolo 8, che stabilisce che ognuno ha il diritto alla protezione dei dati personali che lo riguardano.

(9) Le misure di cui al presente regolamento sono conformi al parere del comitato istituito dall'articolo 20 del regolamento (UE) n. 211/2011,

[1] GU L 65 dell'11.3.2011, pag. 1.

[2] GU L 281 del 23.11.1995, pag. 31.

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Le specifiche tecniche, di cui all'articolo 6, paragrafo 5, del regolamento (UE) n. 211/2011, sono riportate in allegato.

Articolo 2

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 17 novembre 2011

Per la Commissione
Il presidente
José Manuel BARROSO

ALLEGATO

1. SPECIFICHE TECNICHE VOLTE AD ATTUARE L'ARTICOLO 6, PARAGRAFO 4, LETTERA a), DEL REGOLAMENTO (UE) N. 211/2011

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.

2. SPECIFICHE TECNICHE VOLTE AD ATTUARE L'ARTICOLO 6, PARAGRAFO 4, LETTERA b), DEL REGOLAMENTO (UE) N. 211/2011

Norme relative alla sicurezza delle informazioni

2.1. Gli organizzatori 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.

2.2. In base all'analisi dei rischi di cui al punto 2.1, lettera a), 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 presente regolamento di applicazione;

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 per via elettronica. 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.

Requisiti funzionali

2.3. Il sistema di raccolta per via elettronica è costituito da un'istanza applicativa basata su web creata allo scopo di raccogliere le dichiarazioni di sostegno per un'unica iniziativa dei cittadini.

2.4. Se la gestione del sistema richiede diversi ruoli, i differenti livelli di controllo degli accessi sono stabiliti in base al principio del privilegio minimo.

2.5. 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.

2.6. Il sistema rileva e impedisce la duplice trasmissione delle dichiarazioni di sostegno.

Sicurezza a livello dell'applicazione

2.7. Il sistema è adeguatamente protetto contro le vulnerabilità e gli attacchi conosciuti. A tal fine il sistema soddisfa, tra l'altro, i requisiti indicati di seguito.

2.7.1. 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. A tal fine, i requisiti minimi da soddisfare sono i seguenti:

a) tutti i dati di input forniti dagli utenti sono validati;

b) la convalida è effettuata almeno applicando la logica lato server;

c) 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.

2.7.2. Il sistema è protetto contro il Cross-Site Scripting (XSS). A tal fine, i requisiti minimi da soddisfare sono i seguenti:

a) tutti i dati di input forniti dall'utente e rinviati al browser sono controllati sotto il profilo della sicurezza (attraverso una validazione degli input);

b) tutti i dati di input forniti dall'utente sono sottoposti ad una adeguata sequenza di escape prima di essere ripresi nella pagina finale;

c) un'adeguata codifica di output garantisce che tali dati di input siano sempre considerati come testo nel browser. Non sono utilizzati contenuti attivi.

2.7.3. Il sistema ha una rigorosa gestione delle autenticazioni e delle sessioni, che rispetta i requisiti minimi seguenti:

a) 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;

b) 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)];

c) l'ID di sessione e i dati relativi alla sessione non appaiono nell'URL;

d) l'ID di sessione non è vulnerabile ad attacchi di fissazione di sessione;

e) l'ID di sessione ha un tempo di validità (ID timeout), che garantisce la disconnessione degli utenti;

f) gli ID di sessione non sono rinnovati dopo un'autenticazione riuscita;

g) le password, gli ID di sessione e le altre credenziali sono trasmessi soltanto su connessioni TLS (Transport Layer Security);

h) 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 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.

2.7.4. Il sistema non ha riferimenti diretti a oggetti non sicuri. A tal fine, i requisiti minimi da soddisfare sono i seguenti:

a) 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;

b) se il riferimento è di tipo indiretto, il mapping al riferimento diretto è limitato ai valori autorizzati per l'utente corrente.

2.7.5. Il sistema protegge contro gli attacchi di tipo CSRF (Cross Site Request Forgery).

2.7.6. 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.

2.7.7. Il sistema prevede la cifratura dei dati che rispetta i requisiti minimi seguenti:

a) 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;

b) sono utilizzati algoritmi standard e chiavi di cifratura robusti, in linea con gli standard internazionali. Esiste una gestione delle chiavi;

c) le password sono protette da algoritmi standard di hash robusti che utilizzano adeguati parametri salt;

d) tutte le chiavi e le password sono protette da accessi non autorizzati.

2.7.8. Il sistema limita l'accesso agli indirizzi URL in base ai livelli e ai permessi di accesso degli utenti. A tal fine, i requisiti minimi da soddisfare sono i seguenti:

a) 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;

b) se è utilizzata una protezione a livello di codice, la protezione è applicata per tutte le pagine richieste.

2.7.9. Il sistema utilizza una sufficiente protezione del livello di trasporto. A tal fine, devono essere adottate tutte le misure seguenti o misure altrettanto robuste:

a) 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;

b) il flag «secure» deve essere impostato per tutti i cookie riservati;

c) 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.

2.7.10. Il sistema protegge contro reindirizzamenti automatici non validati.

Sicurezza della base dati e integrità dei dati

2.8. Sebbene i sistemi di raccolta per via elettronica 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. Lo stesso vale per la valutazione dei rischi e le contromisure attuate.

2.9. Il rischio che una persona si identifichi nella base dati utilizzando lo strumento «pass-the-hash» è attenuato.

2.10. I dati forniti dai firmatari sono accessibili soltanto all'amministratore/organizzatore della banca dati.

2.11. 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.

2.12. 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.

2.13. 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).

2.14. 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.

2.15. Il sistema di gestione di basi dati (DBMS) utilizzato è costantemente aggiornato con nuove patch contro le vulnerabilità scoperte di recente.

2.16. 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.

Sicurezza delle infrastrutture — ubicazione fisica, infrastrutture di rete e ambiente server

2.17. *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.

2.18. *Sicurezza della rete*

2.18.1. Il sistema è ospitato su un server connesso a Internet installato in una zona demilitarizzata e protetto da un firewall.

2.18.2. Quando vengono resi pubblici aggiornamenti e patch pertinenti al prodotto firewall, tali aggiornamenti o patch sono tempestivamente installati.

2.18.3. Tutto il traffico in entrata e in uscita dal server (destinato al sistema di raccolta per via elettronica) 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.

2.18.4. Il sistema di raccolta per via elettronica 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.

2.18.5. 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.

2.19. *Sicurezza del sistema operativo e del server di rete/dell'applicazione*

2.19.1. È impostata una corretta configurazione di sicurezza, compresi gli elementi elencati al punto 2.7.6.

2.19.2. Le applicazioni funzionano con il minimo dei privilegi necessari.

2.19.3. La sessione di accesso dell'amministratore all'interfaccia di gestione del sistema di raccolta per via elettronica ha un breve tempo di validità (massimo 15 minuti).

2.19.4. 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.

2.19.5. Il rischio che una persona si identifichi nel sistema utilizzando lo strumento «pass-the-hash» è attenuato.

2.20. *Sicurezza organizzatore cliente*

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 per via elettronica e per accedervi, ad esempio:

2.20.1. Gli utenti eseguono compiti non attinenti alla manutenzione (quale l'automazione d'ufficio) con i privilegi minimi necessari.

2.20.2. 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.

3. SPECIFICHE TECNICHE VOLTE AD ATTUARE L'ARTICOLO 6, PARAGRAFO 4, LETTERA c), DEL REGOLAMENTO (UE) N. 211/2011

3.1. 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.

3.2. 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.

3.3. Le dichiarazioni di sostegno esportate verso lo Stato membro interessato sono contrassegnate dalla dicitura «*diffusione limitata*», e classificate come «*dati personali*».

3.4. La trasmissione elettronica dei dati esportati agli Stati membri è protetta da intercettazioni mediante cifratura da punto a punto.