II

(Acte fără caracter legislativ)

REGULAMENTE

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) NR. 1179/2011 AL COMISIEI

din 17 noiembrie 2011

de stabilire a unor specificații tehnice pentru sistemele de colectare online în conformitate cu Regulamentul (UE) nr. 211/2011 al Parlamentului European și al Consiliului privind inițiativa cetățenească

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) nr. 211/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 privind inițiativa cetățenească [1], în special articolul 6 alineatul (5),

după consultarea Autorității Europene pentru Protecția Datelor,

întrucât:

(1) Regulamentul (UE) nr. 211/2011 prevede că atunci când declarațiile de susținere sunt colectate online, sistemul utilizat în acest scop trebuie să îndeplinească anumite cerințe tehnice și de securitate și trebuie să fie certificat de autoritatea competentă a statului membru în cauză.

(2) Un sistem de colectare online în sensul Regulamentului (UE) nr. 211/2011 este un sistem informațional constând din programe, echipamente, mediu de găzduire, procese operaționale și personal, destinat colectării online a declarațiilor de susținere.

(3) Regulamentul (UE) nr. 211/2011 stabilește cerințele pe care trebuie să le respecte sistemele de colectare online în scopul certificării și prevede adoptarea de către Comisie a unor specificații tehnice pentru punerea în aplicare a acestor cerințe.

(4) Proiectul „Top 10 2010" al *Open Web Application Security Project* (OWASP) oferă o prezentare generală a celor mai importante riscuri de securitate ale aplicațiilor web, precum și instrumente pentru contracararea acestor riscuri; specificațiile tehnice se bazează, așadar, pe constatările acestui proiect.

(5) Punerea în aplicare, de către organizatori, a specificațiilor tehnice ar trebui să asigure certificarea sistemelor de colectare online de către autoritățile statelor membre și să contribuie la asigurarea punerii în aplicare a măsurilor tehnice și organizatorice corespunzătoare, necesare pentru a se conforma obligațiilor ce le revin în temeiul Directivei 95/46/CE a Parlamentului European și al Consiliului [2] privind securitatea activităților de prelucrare, atât în momentul proiectării sistemului de prelucrare, cât și în cel al prelucrării în sine, în vederea menținerii securității, prevenind prin aceasta orice prelucrare neautorizată și protejând datele cu caracter personal împotriva distrugerii accidentale sau ilegale sau împotriva pierderii accidentale, modificării, divulgării sau accesului neautorizat.

(6) Procesul de certificare ar trebui să fie facilitat prin folosirea de către organizatori a programului informatic furnizat de Comisie în conformitate cu articolul 6 alineatul (2) din Regulamentul (UE) nr. 211/2011.

(7) Atunci când colectează online declarațiile de susținere, organizatorii inițiativelor cetățenești, în calitate de operatori de date, trebuie să pună în aplicare specificațiile tehnice stabilite în prezentul regulament, astfel încât să asigure protecția datelor personale prelucrate. În cazul în care prelucrarea se efectuează de către un prelucrător, organizatorii trebuie să asigure că acesta acționează exclusiv în conformitate cu instrucțiunile primite de la organizatori și că pune în aplicare specificațiile tehnice stabilite în prezentul regulament.

(8) Prezentul regulament respectă drepturile fundamentale și principiile consacrate în Carta Drepturilor Fundamentale a Uniunii Europene, în special articolul 8, care prevede că orice persoană are dreptul la protecția datelor cu caracter personal care o privesc.

(9) Măsurile prevăzute în prezentul regulament sunt conforme cu avizul Comitetului înființat în baza articolului 20 din Regulamentul (UE) nr. 211/2011,

[1] JO L 65, 11.3.2011, p. 1.

[2] JO L 281, 23.11.1995, p. 31.

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Specificațiile tehnice menționate la articolul 6 alineatul (5) din Regulamentul (UE) nr. 211/2011 sunt prevăzute în anexă.

Articolul 2

Prezentul regulament intră în vigoare în a 20-a zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 17 noiembrie 2011.

Pentru Comisie
Președintele
José Manuel BARROSO

ANEXĂ

1. SPECIFICAȚII TEHNICE PENTRU PUNEREA ÎN APLICARE A ARTICOLULUI 6 ALINEATUL (4) LITERA (a) DIN REGULAMENTUL (UE) NR. 211/2011

Pentru a preveni depunerea automată a unei declarații de susținere prin intermediul sistemului, semnatarul trece printr-un proces adecvat de verificare, în conformitate cu practica actuală, înainte de depunerea unei declarații de susținere. Un posibil proces de verificare constă în utilizarea unui „captcha" puternic.

2. SPECIFICAȚII TEHNICE PENTRU PUNEREA ÎN APLICARE A ARTICOLULUI 6 ALINEATUL (4) LITERA (b) DIN REGULAMENTUL (UE) NR. 211/2011

Norme de siguranță a informațiilor

2.1. Organizatorii furnizează documentație care să precizeze că îndeplinesc cerințele standardului ISO/IEC 27001, fără obligația adoptării acestuia. În acest scop, organizatorii:

(a) au efectuat o evaluare completă a riscurilor, care identifică acoperirea sistemului, indică efectele asupra activității în cazul diferitelor încălcări ale siguranței informațiilor, enumeră amenințările și vulnerabilitățile sistemului informațional, furnizează un document de analiză de risc care indică, de asemenea, măsurile de contracarare a amenințărilor respective și măsurile corective care vor fi aplicate în cazul manifestării unei amenințări și care, în cele din urmă, stabilește o listă de îmbunătățiri enumerate în ordinea priorității;

(b) au conceput și pus în aplicare măsuri pentru tratarea riscurilor cu privire la protecția datelor cu caracter personal și la protecția vieții private și familiale, precum și măsurile care trebuie luate în cazul în care se manifestă aceste riscuri;

(c) au identificat riscuri reziduale în scris;

(d) au precizat mijlocelele organizaționale de primire a feedback-ului privind noile amenințări și îmbunătățirea elementelor de securitate.

2.2. Pe baza analizei de risc de la punctul 2.1 litera (a), organizatorii aleg măsuri de securitate din cadrul standardelor următoare:

1. ISO/IEC 27002; sau

2. „*Standard of Good Practice*", publicat de *Information Security Forum*

pentru abordarea următoarelor aspecte:

(a) evaluări ale riscurilor (sunt recomandate ISO/IEC 27005 sau alte metodologii specifice și adecvate de evaluare a riscurilor);

(b) securitatea fizică și a mediului;

(c) securitatea resurselor umane;

(d) gestionarea comunicațiilor și operațiunilor;

(e) măsuri standard de control al accesului, în plus față de cele stabilite în prezentul regulament de punere în aplicare;

(f) achiziția, dezvoltarea și întreținerea sistemelor informatice;

(g) gestionarea incidentelor de securitate a informațiilor;

(h) măsuri de remediere și contracarare a pătrunderii în sistemele informatice care ar putea duce la distrugerea sau pierderea accidentală, modificarea, accesul ori divulgarea neautorizată a datelor cu caracter personal prelucrate;

(i) conformitate;

(j) securitatea rețelei informatice (sunt recomandate ISO/IEC 27033 sau SoGP).

Aplicarea acestor standarde poate fi limitată la acele secțiuni ale organizației care sunt relevante pentru sistemul de colectare online. De exemplu, securitatea resurselor umane poate fi limitată la membrii personalului care au acces fizic sau în rețea la sistemul de colectare online, iar securitatea fizică/a mediului poate fi limitată la clădirea (clădirile) care găzduiește (găzduiesc) sistemul.

Cerințe funcționale

2.3. Sistemul de colectare online constă dintr-o instanță a unei aplicații web care a fost creată pentru colectarea declarațiilor de susținere a unei inițiative cetățenești unice.

2.4. Dacă gestionarea sistemului necesită diferite roluri, se stabilesc niveluri diferite de control al accesului pe baza principiului celui mai mic privilegiu.

2.5. Elementele accesibile publicului trebuie să fie separate în mod clar de elementele destinate unor scopuri de administrare. Controlul accesului nu împiedică lectura informațiilor disponibile în zona publică a sistemului, inclusiv a informațiilor privind inițiativa și a formularului electronic al declarației de susținere. Înscrierea pentru susținerea unei inițiative este posibilă numai prin această zonă publică.

2.6. Sistemul detectează și previne introducerea unor duplicate ale declarațiilor de susținere.

Securitatea la nivelul aplicației informatice

2.7. Sistemul este protejat corespunzător împotriva vulnerabilităților și exploatărilor de deficiențe care sunt cunoscute. În acest scop el îndeplinește, printre altele, următoarele cerințe:

2.7.1. Sistemul oferă protecție împotriva atacurilor de tipul „*injection flaw*”, cum ar fi prin interogări lansate în *Structured Query Language* (SQL), *Lightweight Directory Access Protocol* (LDAP), *XML Path Language* (XPath), prin comenzi de sistem de operare (OS) sau prin argumente de program. În acest scop, impune cel puțin că:

(a) toate instrucțiunile din partea utilizatorului sunt validate;

(b) validarea este efectuată, cel puțin, de aplicațiile de pe server;

(c) orice utilizare a interpretorilor separă în mod clar datele nesigure de partea de comandă sau de interogare. Pentru apeluri SQL, aceasta înseamnă utilizarea variabilelor obligatorii în toate rapoartele pregătite și procedurile stocate, precum și evitarea interogărilor dinamice.

2.7.2. Sistemul oferă protecție împotriva *Cross-Site Scripting* (XSS). În acest scop, impune cel puțin că:

(a) toate datele de intrare furnizate, retransmise către browser, sunt verificate ca fiind sigure (prin validarea datelor de intrare);

(b) toate datele introduse de utilizator sunt formatate în mod corespunzător înainte de a fi incluse în pagina de afișare;

(c) formatarea adecvată a afișării garantează că datele de intrare sunt întotdeauna tratate ca text în browser. Nu se folosește conținut activ.

2.7.3. Sistemul oferă autentificare și gestionare de sesiune puternice, care prevăd cel puțin că:

(a) datele de acreditare sunt întotdeauna protejate prin hashing sau criptare atunci când sunt stocate. Riscul ca cineva să se autentifice prin tehnica „pass-the-hash” este contracarat;

(b) datele de acreditare nu pot fi ghicite sau rescrise prin intermediul unor funcții slabe de administrare a contului [cum ar fi crearea de conturi, schimbarea parolei, recuperarea parolei, identificatori de sesiune (ID-uri) slabi];

(c) ID-urile de sesiune și datele de sesiune nu sunt expuse în *Uniform Resource Locator* (URL);

(d) ID-urile de sesiune nu sunt vulnerabile la atacuri de tipul „*session fixation*”;

(e) ID-urile de sesiune expiră, ceea ce asigură deconectarea utilizatorilor;

(f) ID-urile de sesiune nu sunt refolosite după efectuarea unei conectări;

(g) parolele, ID-urile de sesiune și celelalte elemente de acreditare sunt transmise numai prin *Transport Layer Security* (TLS);

(h) partea de gestionare a sistemului este protejată. În cazul în care este protejată prin autentificare pe baza unui singur factor, parola este formată din cel puțin 10 caractere, incluzând cel puțin o literă, un număr și un caracter special. Ca alternativă, poate fi utilizată autentificarea pe baza a doi factori. În cazul în care se utilizează doar autentificarea pe baza unui singur factor, aceasta include un mecanism de verificare în două etape pentru accesarea părții de gestionare a sistemului prin internet, în care factorului respectiv i se adaugă un alt mijloc de identificare, cum ar fi un cod de unică folosință sau un cod prin SMS, ori un șir aleatoriu criptat asimetric și care trebuie decriptat cu cheia privată a organizatorilor/administratorilor, aceasta fiind necunoscută de sistem.

2.7.4. Sistemul nu conține referințe directe nesecurizate către obiecte („*insecure direct object references*"). În acest scop, impune cel puțin că:

(a) pentru referințe directe către resurse restricționate, aplicația verifică dacă utilizatorul este autorizat să aibă acces la resursele solicitate respective;

(b) dacă referința este una indirectă, maparea la referința directă este limitată la valorile autorizate pentru utilizatorul curent.

2.7.5. Sistemul oferă protecție împotriva falsificării cererilor între site-uri („*cross-site request forgery*").

2.7.6. Există o configurație corespunzătoare de securitate, care necesită, cel puțin, ca:

(a) toate componentele software să fie actualizate, inclusiv OS, serverul web/de aplicații, sistemul de gestionare a bazei de date (DBMS), aplicațiile și toate bibliotecile de cod;

(b) serviciile care nu sunt necesare din cadrul OS și de pe serverul web/de aplicații sunt dezactivate, dezinstalate sau neinstalate;

(c) parolele implicite ale conturilor sunt schimbate sau dezactivate;

(d) sistemul de gestionare a erorilor este configurat pentru a preveni comunicarea informațiilor din stivă și comunicarea altor mesaje de eroare prea informative;

(e) setările de securitate în mediile și bibliotecile de dezvoltare sunt configurate în conformitate cu bunele practici, cum ar fi orientările OWASP.

2.7.7. Sistemul prevede criptarea datelor după cum urmează:

(a) datele cu caracter personal în format electronic sunt criptate când sunt stocate sau transferate către autoritățile competente ale statelor membre, în conformitate cu articolul 8 alineatul (1) din Regulamentul (UE) nr. 211/2011, administrarea și copia de rezervă a cheilor fiind făcute separat;

(b) se folosesc algoritmi standard puternici, precum și chei puternice, în conformitate cu standardele internaționale. Există o procedură de gestionare a cheilor;

(c) parolele sunt criptate cu un algoritm standard puternic și se utilizează o valoare aleatorie („*salt*") adecvată;

(d) toate cheile și parolele sunt protejate împotriva accesului neautorizat.

2.7.8. Sistemul restrânge accesul URL pe baza nivelurilor și permisiunilor de acces ale utilizatorilor. În acest scop, impune cel puțin că:

(a) în cazul în care se folosesc mecanisme de securitate externe pentru a realiza autentificarea și autorizarea accesului la pagini, aceste mecanisme trebuie să fie corect configurate pentru fiecare pagină;

(b) în cazul în care se folosește protecție la nivelul codului, trebuie să existe protecție la nivel de cod pentru fiecare pagină solicitată.

2.7.9. Sistemul utilizează *Transport Layer Protection* la un nivel suficient. În acest scop, sunt aplicate toate măsurile următoare, ori măsuri cu grad de siguranță cel puțin echivalent:

(a) sistemul necesită cea mai recentă versiune a protocolului de transfer hipertext securizat (HTTPS) pentru accesul la orice resursă sensibilă pe baza unor certificate valabile, care nu au expirat și nu sunt revocate, pentru toate domeniile utilizate de site;

(b) sistemul setează opțiunea „secure" pentru toate cookie-urile sensibile;

(c) serverul configurează furnizorul TLS astfel încât să funcționeze numai cu algoritmi de criptare care respectă cele mai bune practici. Utilizatorii sunt informați că browser-ul lor trebuie să permită utilizarea TLS.

2.7.10. Sistemul oferă protecție împotriva redirectărilor și *forward*-urilor invalidate.

Securitatea bazei de date și integritatea datelor

2.8. În cazul în care sistemele de colectare online utilizate pentru inițiative cetățenești diferite folosesc echipamente și resurse ale sistemului de operare comune, ele nu au acces comun la niciun element al datelor, inclusiv la elementele de acreditare pentru acces/criptare. În plus, acest lucru este reflectat în evaluarea riscurilor și în măsurile de contracarare puse în aplicare.

2.9. Riscul ca cineva să se autentifice în baza de date utilizând tehnica „pass-the-hash" este contracarat.

2.10. Datele furnizate de către semnatari sunt accesibile numai administratorului bazei de date/organizatorului.

2.11. Elementele de acreditare pentru administrare, datele cu caracter personal colectate de la semnatari, precum și copiile de rezervă ale acestora sunt protejate prin algoritmi de criptare puternici în conformitate cu punctul 2.7.7 litera (b). Cu toate acestea, statul membru în care declarația de susținere va fi numărată, data depunerii declarației de susținere și limba în care semnatarul a completat formularul de declarație de susținere pot fi stocate în sistem fără a fi criptate.

2.12. Semnatarii au acces doar la datele transmise în cursul sesiunii în care completează formularul de declarație de susținere. Odată ce formularul de declarație de susținere este trimis, sesiunea respectivă este închisă și datele trimise nu mai sunt accesibile.

2.13. Datele cu caracter personal ale semnatarilor, inclusiv copia de rezervă, sunt disponibile în sistem doar în formă criptată. În scopul consultării sau certificării datelor de către autoritățile naționale în conformitate cu articolul 8 din Regulamentul (UE) nr. 211/2011, organizatorii pot exporta datele criptate în conformitate cu punctul 2.7.7 litera (a).

2.14. Persistența datelor introduse în formularul de declarație de susținere este atomică. Aceasta înseamnă că, odată ce utilizatorul a introdus toate detaliile solicitate în formularul de declarație de susținere și și-a validat decizia de a sprijini inițiativa, sistemul fie transmite cu succes toate datele din formular către baza de date, fie, în caz de eroare, nu înregistrează niciun element din datele respective. Sistemul informează utilizatorul despre reușita sau eșecul operațiunii.

2.15. DBMS utilizat este actualizat și protejat continuu față de ultimele amenințări descoperite.

2.16. Toate jurnalele de activitate ale sistemului sunt activate. Sistemul asigură faptul că jurnalele de audit care înregistrează excepțiile și alte evenimente relevante pentru securitate, enumerate mai jos, pot fi disponibile și păstrate până în momentul în care datele sunt distruse în conformitate cu articolul 12 alineatul (3) sau (5) din Regulamentul (UE) nr. 211/2011. Jurnalele sunt protejate în mod corespunzător, de exemplu prin stocare pe medii criptate. Organizatorii/administratorii verifică în mod regulat jurnalele pentru depistarea activităților suspecte. Jurnalele conțin cel puțin:

(a) datele și orele conectării și deconectării organizatorilor/administratorilor;

(b) copiile de rezervă efectuate;

(c) toate modificările și actualizările referitoare la administratorul bazei de date.

Siguranța infrastructurilor – amplasamentul fizic, infrastructura de rețea și mediul serverului

2.17. *Securitatea fizică*

Indiferent de tipul de găzduire utilizat, mașină care găzduiește aplicația este protejată în mod corespunzător, ceea ce presupune:

(a) un control al accesului și un jurnal de audit pentru zona de găzduire;

(b) protecția fizică a datelor de rezervă împotriva furturilor sau pierderii accidentale;

(c) serverul care găzduiește aplicația este instalat într-un stativ securizat.

2.18. *Securitatea rețelelor*

2.18.1. Sistemul este găzduit pe un server internet instalat într-o „zonă demilitarizată" (DMZ) și protejat de un firewall.

2.18.2. În momentul în care actualizările și corecțiile programului firewall devin publice, acestea sunt instalate fără întârziere.

2.18.3. Tot traficul de intrare și de ieșire al serverului (destinat sistemului de colectare online) este inspectat de regulile programului firewall și înregistrat în jurnal. Regulile programului firewall refuza orice trafic ce nu este necesar pentru utilizarea și administrarea securizată a sistemului.

2.18.4. Sistemul de colectare online trebuie să fie găzduit pe un segment de rețea de producție protejat în mod adecvat, separat de segmentele utilizate pentru găzduirea sistemelor nedestinate producției, cum ar fi mediile de dezvoltare sau de testare.

2.18.5. Sunt aplicate măsuri de securitate pentru rețeaua locală (LAN), cum ar fi:

(a) listă de acces nivel 2 (L2)/securitatea porturilor din switch;

(b) porturile din switch neutilizate sunt dezactivate;

(c) DMZ se află pe o rețea locală virtuală dedicată (VLAN)/LAN;

(d) nu se activează L2 trunking pe porturile pe care acest lucru nu este necesar.

2.19. *Securitatea OS și a serverului web/de aplicații*

2.19.1. Este utilizată o configurație de siguranță adecvată, inclusiv elementele enumerate la punctul 2.7.6

2.19.2. Aplicațiile rulează cu cel mai restrâns set de privilegii necesar pentru funcționare.

2.19.3. Accesul administratorului la interfața de gestionare a sistemului de colectare online expiră după o sesiune scurtă (maxim 15 minute).

2.19.4. În cazul în care actualizările și corecțiile relevante ale OS, ale aplicațiilor runtime, ale aplicațiilor rulând pe servere sau ale programelor anti-malware devin publice, aceste actualizări sau corecții sunt instalate fără întârziere.

2.19.5. Riscul ca cineva să se autentifice în sistem utilizând tehnica „pass-the-hash" este contracarat.

2.20. *Securitatea clientului organizatorului*

Din motive de securitate de-a lungul întregului proces, organizatorii adoptă măsurile necesare pentru a securiza aplicația/dispozitivul client folosit(ă) pentru gestionarea și accesarea sistemului de colectare online, cum ar fi:

2.20.1. utilizatorii rulează sarcini care nu sunt de întreținere (de exemplu, birotică) cu cel mai mic set de privilegii necesar pentru funcționare;

2.20.2. în cazul în care actualizările și corecțiile relevante ale OS, ale oricăror aplicații instalate sau ale programelor anti-malware devin publice, aceste actualizări sau corecții sunt instalate fără întârziere.

3. SPECIFICAȚII TEHNICE PENTRU PUNEREA ÎN APLICARE A ARTICOLULUI 6 ALINEATUL (4) LITERA (c) DIN REGULAMENTUL (UE) NR. 211/2011

3.1. Sistemul prevede posibilitatea de a extrage pentru fiecare stat membru un raport care să cuprindă inițiativa și datele cu caracter personal ale semnatarilor pentru verificarea de către autoritatea competentă din statul membru în cauză.

3.2. Exportarea declarațiilor de susținere ale semnatarilor este posibilă în formatul din anexa III la Regulamentul nr. 211/2011. Sistemul poate să prevadă, de asemenea, posibilitatea de exportare a declarațiilor de susținere într-un format interoperabil, cum ar fi XML (*Extensible Markup Language*).

3.3. Declarațiile de susținere exportate sunt marcate ca fiind cu *distribuție limitată* pentru statul membru în cauză și clasificate ca *date cu caracter personal*.

3.4. Transmiterea electronică a datelor exportate către statele membre este protejată împotriva interceptărilor prin criptare adecvată de-a lungul întregului proces.