II

*(Nelegislatívne akty)*

# NARIADENIA

## VYKONÁVACIE NARIADENIE KOMISIE (EÚ) č. 1179/2011

**zo 17. novembra 2011,**

**ktorým sa ustanovujú technické špecifikácie pre elektronické systémy zberu podľa nariadenia Európskeho parlamentu a Rady (EÚ) č. 211/2011 o iniciatíve občanov**

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) č. 211/2011 zo 16. februára 2011 o iniciatíve občanov [1], a najmä na jeho článok 6 ods. 5,

po konzultácii s európskym dozorným úradníkom pre ochranu údajov,

keďže:

(1) Nariadenie (EÚ) č. 211/2011 stanovuje, že ak sa vyhlásenia o podpore zbierajú elektronicky, systém použitý na tento účel musí spĺňať určité bezpečnostné a technické požiadavky a musí mať osvedčenie od príslušného orgánu dotknutého členského štátu.

(2) Elektronický systém zberu v zmysle nariadenia (EÚ) č. 211/2011 je informačný systém, ktorý sa skladá zo softvéru, hardvéru, hostiteľského prostredia, obchodných postupov a personálu a ktorého cieľom je vykonávať elektronický zber vyhlásení o podpore.

(3) Nariadenie (EÚ) č. 211/2011 vymedzuje požiadavky, ktoré musia elektronické systémy zberu splniť, aby dostali osvedčenie, a stanovuje, že Komisia by mala prijať technické špecifikácie na vykonávanie týchto požiadaviek.

(4) Projekt Top 10 2010 OWASP (Open Web Application Security Project) poskytuje prehľad najvážnejších bezpečnostných rizík webových aplikácií a tiež nástroje na riešenie týchto rizík; technické špecifikácie preto vychádzajú zo záverov tohto projektu.

(5) Vykonávanie technických špecifikácií zo strany organizátorov by malo zaručiť osvedčenie elektronických systémov zberu orgánmi členských štátov a malo by pomôcť zabezpečiť vykonávanie príslušných technických a organizačných opatrení potrebných na splnenie povinností stanovených smernicou Európskeho parlamentu a Rady 95/46/ES [2] o bezpečnosti spracovania v čase návrhu systému spracovania a v čase samotného spracovania, aby sa udržala bezpečnosť a predišlo sa tým akémukoľvek nedovolenému spracovaniu a aby sa zabezpečila ochrana osobných údajov pred náhodným alebo nezákonným zničením alebo náhodnou stratou, zmenou, neoprávneným sprístupnením alebo prístupom.

(6) Využívanie softvéru poskytnutého Komisiou v súlade s článkom 6 ods. 2 nariadenia (EÚ) č. 211/2011 zo strany organizátorov by malo uľahčiť postup osvedčovania.

(7) Organizátori iniciatív občanov by ako prevádzkovatelia údajov mali pri elektronickom zbere vyhlásení o podpore vykonávať technické špecifikácie stanovené v tomto nariadení s cieľom zabezpečiť ochranu spracúvaných osobných údajov. Keď spracúvanie vykonáva spracovateľ, organizátori by mali zabezpečiť, aby spracovateľ konal len na základe pokynov organizátorov a aby vykonával technické špecifikácie stanovené v tomto nariadení.

(8) Toto nariadenie rešpektuje základné práva a dodržiava zásady stanovené v Charte základných práv Európskej únie, osobitne v článku 8, v ktorom je uvedené, že každý má právo na ochranu osobných údajov, ktoré sa ho týkajú.

(9) Opatrenia ustanovené v tomto nariadení sú v súlade so stanoviskom výboru zriadeného podľa článku 20 nariadenia (EÚ) č. 211/2011,

[1] Ú. v. EÚ L 65, 11.3.2011, s. 1.

[2] Ú. v. ES L 281, 23.11.1995, s. 31.

PRIJALA TOTO NARIADENIE:

*Článok 1*

Technické špecifikácie uvedené v článku 6 ods. 5 nariadenia (EÚ) č. 211/2011 sú stanovené v prílohe.

*Článok 2*

Toto nariadenie nadobúda účinnosť dvadsiaty deň po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 17. novembra 2011

*Za Komisiu*
*predseda*
José Manuel BARROSO

*PRÍLOHA*

1. TECHNICKÉ ŠPECIFIKÁCIE, KTORÝCH ÚČELOM JE VYKONÁVANIE ČLÁNKU 6 ODS. 4 PÍSM. a) NARIADENIA (EÚ) č. 211/2011

S cieľom zabrániť automatizovanému predloženiu vyhlásenia o podpore využitím systému absolvuje signatár pred predložením vyhlásenia o podpore primeraný proces verifikácie. Jedným z možných spôsobov verifikácie je využitie účinného testu „captcha".

2. TECHNICKÉ ŠPECIFIKÁCIE, KTORÝCH ÚČELOM JE VYKONÁVANIE ČLÁNKU 6 ODS. 4 PÍSM. b) NARIADENIA (EÚ) č. 211/2011

**Normy zabezpečenia informácií**

2.1. Organizátori pred schválením predložia dokumentáciu, ktorá preukazuje, že spĺňajú požiadavky normy ISO/IEC 27001, okrem jej prijatia. Na tento účel musia:

a) vykonať úplné hodnotenie rizika, v ktorom sa určí rozsah systému, vyzdvihne sa obchodný dosah v prípade rôznych narušení zabezpečenia informácií, uvedú sa riziká a slabé stránky informačného systému, vypracuje sa dokument s analýzou rizika, v ktorom budú uvedené aj protiopatrenia na zabránenie takýmto rizikám a nápravné prostriedky, ktoré sa prijmú v prípade výskytu rizika, a napokon sa vypracuje zoznam vylepšení v poradí podľa priorít;

b) navrhnúť a zaviesť opatrenia na riešenie rizík súvisiacich s ochranou osobných údajov a ochranou rodinného a súkromného života a opatrenia, ktoré sa prijmú v prípade výskytu rizika;

c) v písomnej forme určiť reziduálne riziká;

d) zabezpečiť organizačné prostriedky na získanie spätnej väzby, pokiaľ ide o nové riziká a vylepšenia bezpečnosti.

2.2. Organizátori si zvolia opatrenia na kontrolu bezpečnosti na základe analýzy rizika uvedenej v bode 2.1. písm. a) z týchto noriem:

1. ISO/IEC 27002 alebo

2. „Štandard osvedčených postupov" Fóra informačnej bezpečnosti

na riešenie týchto záležitostí:

a) hodnotenie rizík (odporúča sa ISO/IEC 27005 alebo iná špecifická a vhodná metodika posudzovania rizika);

b) fyzická a environmentálna bezpečnosť;

c) bezpečnosť ľudských zdrojov;

d) riadenie komunikácie a operácií;

e) štandardné opatrenia na kontrolu prístupu popri opatreniach uvedených v tomto vykonávacom nariadení;

f) nadobudnutie, rozvoj a údržba informačných systémov;

g) riadenie prípadov narušenia bezpečnosti informácií;

h) opatrenia na nápravu a zmiernenie narušení informačných systémov, ktoré by viedli k zničeniu alebo náhodnej strate, zmene spracúvaných osobných údajov, ich neoprávnenému sprístupneniu alebo prístupu k nim;

i) súlad;

j) bezpečnosť počítačovej siete (odporúča sa ISO/IEC 27033 alebo štandard osvedčených postupov).

Uplatňovanie týchto noriem môže byť obmedzené na časti organizácie, ktoré súvisia s elektronickým systémom zberu. Napríklad bezpečnosť ľudských zdrojov môže byť obmedzená na personál, ktorý má fyzický alebo sieťový prístup k elektronickému systému zberu, a fyzická/environmentálna bezpečnosť môže byť obmedzená na budovy, v ktorých je systém umiestnený.

**Funkčné požiadavky**

2.3. Elektronický systém zberu pozostáva z webovej aplikácie vytvorenej na účely zberu vyhlásení o podpore pre jednu iniciatívu občanov.

2.4. Ak sú na správu systému potrebné rôzne úlohy, vytvoria sa rôzne úrovne riadenia prístupu podľa princípu najnižších práv.

2.5. Verejne prístupné funkcie sú jasne oddelené od funkcií určených na účely správy. Riadenie prístupu nebráni čítaniu informácií dostupných vo verejnej časti systému vrátane informácií o iniciatíve a o elektronickom formulári vyhlásenia o podpore. Podpísanie iniciatívy je možné len v tejto verejnej časti.

2.6. Systém rozpoznáva predloženie duplicitného vyhlásenia o podpore a zabraňuje tomu.

**Bezpečnosť na úrovni aplikácie**

2.7. Systém je náležite zabezpečený, pokiaľ ide o známe slabé stránky a zneužitie. Na tento účel spĺňa okrem iného tieto požiadavky:

2.7.1. Systém je zabezpečený voči chybám pri vkladaní (injection flaws), ako sú požiadavky štruktúrovaného dopytovacieho jazyka SQL (Structured Query Language), požiadavky protokolu ľahkého prístupu k zoznamu LDAP (Lightweight Directory Access Protocol), požiadavky XPath (XML Path Language), príkazy operačného systému (OS) alebo argumenty programu. Na tento účel je minimálne potrebné:

a) Všetky používateľské vstupy sa overujú.

b) Overovanie sa vykonáva prinajmenšom prostredníctvom logiky na strane servera.

c) Použitie prekladačov jasne oddeľuje nedôveryhodné údaje od príkazu alebo požiadavky. V prípade spojení SQL to znamená využitie väzobných premenných vo všetkých pripravených vyhláseniach a uložených postupoch a vyhnutie sa dynamickým požiadavkám.

2.7.2. Systém je zabezpečený voči XSS (Cross-Site Scripting). Na tento účel je minimálne potrebné:

a) Všetky zadané používateľské vstupy zaslané späť prehliadaču sa overujú, pokiaľ ide o ich bezpečnosť (prostredníctvom kontroly vstupných parametrov).

b) Všetky používateľské vstupy sa vrátia do povelovej úrovne pred začlenením do stránky výstupu.

c) Náležité výstupné kódovanie zabezpečí, aby sa takéto vstupy v prehliadači vždy spracovali ako text. Nepoužíva sa nijaký aktívny obsah.

2.7.3. Systém má silné riadenie overenia totožnosti a relácií, na čo je minimálne potrebné:

a) Prístupové kódy sú pri ukladaní vždy chránené pomocou hašovania alebo šifrovania. Riziko, že sa niekto identifikuje pomocou „pass-the-hash“, je minimalizované.

b) Prístupové kódy sa nemôžu dať uhádnuť alebo prepísať v dôsledku slabých funkcií riadenia účtu [napr. vytvorenie účtu, zmena hesla, získanie zabudnutého hesla, slabé identifikátory relácie (ID)].

c) Identifikátory relácie a údaje o relácií sa nezobrazujú v jednotnom vyhľadávači zdrojov URL (Uniform Resource Locator).

d) Identifikátory relácie sú odolné voči útokom fixovania relácií (session fixation).

e) Časový limit identifikátorov relácie, ktorý zabezpečí odhlásenie používateľov.

f) Identifikátory relácie po úspešnom prihlásení nemôžu rotovať.

g) Heslá, identifikátory relácie a ďalšie prístupové kódy sa zasielajú len prostredníctvom bezpečnostnej prenosovej vrstvy TLS (Transport Layer Security).

h) Administratívna časť systému je zabezpečená. Ak je zabezpečená jednofaktorovým overením totožnosti, heslo obsahuje minimálne 10 znakov, medzi ktorými je najmenej jedno písmeno, jedno číslo a jeden špeciálny znak. Prípadne sa môže použiť dvojfaktorové overenie totožnosti. V prípade, že sa používa len jednofaktorové overenie totožnosti, zahŕňa dvojstupňový mechanizmus overovania pre prístup k administratívnej časti systému cez Internet, v ktorom sa jeden faktor rozšíri o ďalšie prostriedky overenia totožnosti, ako napríklad o jednorazovú kontrolnú vetu/kód cez SMS alebo asymetricky zašifrovaný náhodný reťazec (challenge string), ktorý sa dešifruje prostredníctvom osobného kľúča organizátora/správcu, ktorý je pre systém neznámy.

2.7.4. Systém nemôže mať nezabezpečené odkazy na priame objekty. Na tento účel je minimálne potrebné:

a) v prípade priamych odkazov na obmedzené zdroje aplikácia overiť, či má používateľ autorizovaný prístup k presnému požadovanému zdroju;

b) ak je odkaz nepriamy, mapovanie k priamemu odkazu je obmedzené na hodnoty autorizované pre aktuálneho používateľa.

2.7.5. Systém musí byť zabezpečený proti falšovaniu oprávnených požiadaviek (cross-site request forgery flaw).

2.7.6. Je zabezpečená primeraná konfigurácia bezpečnosti, na čo je minimálne potrebné:

a) Všetky komponenty softvéru sú aktuálne vrátane OS, webového servera/servera aplikácie, databázového systému (DBMS), aplikácií a všetkých kryptografických knižníc.

b) Nepotrebné funkcie OS a webového servera/servera aplikácie sú vypnuté, vymazané alebo nie sú nainštalované.

c) Prednastavené heslá k účtu sa zmenia alebo znefunkčnia.

d) Spracovanie chýb sa nastaví tak, aby zabránilo úniku tzv. stack traces a iných príliš informatívnych chybových hlásení.

e) Bezpečnostné nastavenia vo vývojových štruktúrach a knižniciach sú nakonfigurované v súlade s osvedčenými postupmi, napríklad s usmerneniami OWASP.

2.7.7. Systém zabezpečuje takéto šifrovanie údajov:

a) Osobné údaje v elektronickom formáte sú šifrované pri ukladaní alebo posielaní príslušným orgánom členských štátov v súlade s článkom 8 ods. 1 nariadenia (EÚ) č. 211/2011, kľúče sa spravujú a zálohujú osobitne.

b) Odolné štandardné algoritmy a odolné kľúče sa používajú v súlade s medzinárodnými normami. Zabezpečí sa riadenie kľúčov.

c) Heslá sú hašované prostredníctvom odolného štandardného algoritmu a používa sa primeraný náhodný reťazec – falzifikát (salt).

d) Všetky kľúče a heslá sú zabezpečené pred neoprávneným prístupom.

2.7.8. Systém obmedzuje prístup URL na základe prístupových úrovní používateľa a jeho oprávnení. Na tento účel je minimálne potrebné:

a) Ak sa na zabezpečenie kontrol overenia totožnosti a oprávnenia pre prístup na stránku používajú externé bezpečnostné mechanizmy, musia byť náležite nakonfigurované pre každú stránku.

b) Ak sa používa ochrana na základe úrovne kódu, musí fungovať pre každú požadovanú stránku.

2.7.9. Systém využíva dostatočnú ochranu prenosovej vrstvy (Transport Layer Protection). Na tento účel sú zavedené všetky z týchto opatrení alebo minimálne rovnako silné opatrenia:

a) Systém vyžaduje najnovšiu verziu zabezpečeného hypertextového prenosového protokolu HTTPS (Hypertext Transfer Protocol Secure) na prístup k všetkým citlivým zdrojom použitím certifikátov, ktoré sú platné, neskončila im platnosť, neboli odvolané a zodpovedajú všetkým doménam, ktoré stránka používa.

b) Systém označuje všetky citlivé súbory cookies ako bezpečné.

c) Server nakonfiguruje poskytovateľa TLS, aby podporoval len šifrovacie algoritmy, ktoré zodpovedajú osvedčeným postupom. Používatelia sú informovaní o tom, že musia vo svojom prehliadači umožniť podporu TLS.

2.7.10. Systém poskytuje ochranu pred zrušenými presmerovaniami a prevodmi.

**Bezpečnosť databázy a integrita údajov**

2.8. Ak majú elektronické systémy zberu využívané na rôzne iniciatívy občanov spoločné hardvérové zdroje a zdroje operačného systému, nemôžu spoločne používať nijaké údaje, a to ani prístupové/šifrovacie údaje. Zohľadní sa to aj v hodnotení rizika a prijatých protiopatreniach.

2.9. Riziko, že sa niekto v databáze identifikuje pomocou „pass-the-hash", je minimalizované.

2.10. Údaje, ktoré signatári poskytnú, sú prístupné len pre správcu databázy/organizátora.

2.11. Prístupové kódy správcu, osobné údaje vyzbierané od signatárov a ich záloha sú zabezpečené prostredníctvom odolných šifrovacích algoritmov v súlade s bodom 2.7.7 písm. b). V systéme však môžu byť nezašifrovane uložené tieto údaje: členský štát, ktorého sa týka vyhlásenie o podpore, dátum predloženia vyhlásenia o podpore a jazyk, v ktorom signatár vyplnil vyhlásenie o podpore.

2.12. Signatári majú k poskytnutým údajom prístup len počas relácie, v ktorej vyplnia formulár vyhlásenia o podpore. Po zaslaní vyhlásenia o podpore sa uvedená relácia ukončí a poskytnuté údaje už nie sú prístupné.

2.13. Osobné údaje signatárov sú v systéme vrátane zálohy dostupné len v zašifrovanom formáte. Na účely informovania o údajoch alebo vydania osvedčenia zo strany príslušných orgánov v súlade s článkom 8 nariadenia (EÚ) č. 211/2011 môžu organizátori exportovať šifrované údaje v súlade s bodom 2.7.7 písm. a).

2.14. Stálosť údajov vložených do formulára vyhlásenia o podpore musí byť atomická. To znamená, že po tom, ako používateľ do formulára vyhlásenia o podpore vložil všetky požadované údaje a potvrdil svoje rozhodnutie podporiť iniciatívu, systém buď úspešne vloží všetky údaje z formulára do databázy, alebo v prípade chyby neuloží nijaké údaje. Systém informuje používateľa o úspechu alebo neúspechu jeho požiadavky.

2.15. Používaný databázový systém musí byť aktuálny a musí sa neustále vylepšovať o nové prvky.

2.16. Všetky aktivity systému sa zaznamenávajú. Systém zabezpečí, aby sa kontrolné záznamy so zapísanými výnimkami a ďalšími prípadmi súvisiacimi s bezpečnosťou, ktoré sú uvedené nižšie, mohli predložiť a uchovať, pokým údaje nebudú zničené v súlade s článkom 12 ods. 3 alebo 5 nariadenia (EÚ) č. 211/2011. Záznamy sú primerane chránené, napríklad uložením na zašifrovaných médiách. Organizátori/správcovia záznamy pravidelne kontrolujú v súvislosti s podozrivou aktivitou. Minimálny obsah záznamov:

a) dátumy a časy prihlásenia a odhlásenia organizátorov/správcov;

b) vykonané zálohy;

c) všetky zmeny a aktualizácie správcu databázy.

**Bezpečnosť infraštruktúry – fyzické umiestnenie, sieťová infraštruktúra a prostredie servera**

2.17. *Fyzická bezpečnosť*

Bez ohľadu na typ použitého spôsobu hostiteľstva je zariadenie, ktoré je hostiteľom aplikácie, náležité chránené, čo znamená:

a) kontrola prístupu k oblasti hosťovania a kontrolný záznam;

b) fyzická ochrana zálohovaných údajov pred krádežou alebo náhodným nesprávnym umiestnením;

c) server, ktorý je hostiteľom aplikácie, je nainštalovaný v zabezpečenom nosiči.

2.18. *Bezpečnosť siete*

2.18.1. Systém je umiestnený na internetovom serveri nainštalovanom v demilitarizovanej zóne a je chránený prostredníctvom bezpečnostného rozhrania (firewall).

2.18.2. Keď sa zverejnia príslušné aktualizácie a opravy produktu bezpečnostného rozhrania, náležite sa nainštalujú.

2.18.3. Všetky prenosy na server a zo servera (určené pre elektronický systém zberu) sú kontrolované podľa pravidiel bezpečnostného rozhrania a zaznamenávajú sa. Pravidlá bezpečnostného rozhrania odmietajú všetky prenosy, ktoré nie sú potrebné na bezpečné používanie a správu systému.

2.18.4. Elektronický systém zberu musí byť umiestnený v primerane zabezpečenom produkujúcom segmente siete, ktorý je oddelený od ostatných segmentov používaných na umiestnenie neprodukujúcich systémov, ako napríklad vývoj alebo testovacie prostredia.

2.18.5. Musia sa zaviesť bezpečnostné opatrenia pre miestnu počítačovú sieť (LAN), ako napríklad:

a) zoznam prístupov layer 2 (L2)/bezpečnosť prepínača portov (port switch);

b) nevyužité prepínače portov (switch ports) sa znefunkčnia;

c) DMZ je umiestnená na dedikovanej virtuálnej miestnej počítačovej sieti [Virtual Local Area Network (VLAN)/LAN];

d) na nepotrebných portoch sa neumožňuje tvorba zväzkov (trunking) L2.

2.19. *Bezpečnosť OS a webového servera/servera aplikácie*

2.19.1. Zabezpečí sa primeraná konfigurácia bezpečnosti vrátane prvkov uvedených v bode 2.7.6.

2.19.2. Aplikácie fungujú s najnižším súborom privilégií, ktoré potrebujú na svoje fungovanie.

2.19.3. Prístup správcu k rozhraniu správy elektronického systému zberu má krátky časový limit (maximálne 15 minút).

2.19.4. Keď sa zverejnia príslušné aktualizácie a opravy OS, aplikácií modulov runtime, aplikácií bežiacich na serveroch alebo aplikácií proti škodlivému softvéru, musia byť náležite nainštalované.

2.19.5. Riziko, že niekto sa v databáze identifikuje pomocou „pass-the-hash“, je minimalizované.

2.20. *Bezpečnosť klienta organizátora*

Na zaistenie bezpečnosti po celej dĺžke spojenia organizátori prijmú potrebné opatrenia, aby zabezpečili svoju klientsku aplikáciu/svoje klientske zariadenie, ktoré používajú na správu elektronického systému zberu a prístup k nemu, a to:

2.20.1. Používatelia môžu používať neúdržbové funkcie (ako napríklad automatizácia administratívy) s najnižším súborom privilégií, ktoré sú potrebné na fungovanie.

2.20.2. Keď sa zverejnia príslušné aktualizácie a opravy OS, akýchkoľvek nainštalovaných aplikácií alebo aplikácií proti škodlivému softvéru, náležite sa nainštalujú.

3. TECHNICKÉ ŠPECIFIKÁCIE, KTORÝCH ÚČELOM JE VYKONÁVANIE ČLÁNKU 6 ODS. 4 PÍSM. c) NARIADENIA (EÚ) č. 211/2011

3.1. Systém poskytuje možnosť získať pre jednotlivé členské štáty správu, v ktorej bude uvedená iniciatíva a osobné údaje signatárov podliehajúce overeniu zo strany príslušného orgánu predmetného členského štátu.

3.2. Vyhlásenia signatárov o podpore sa môžu exportovať vo formáte prílohy III k nariadeniu č. 211/2011. Systém môže navyše poskytnúť možnosť exportovať vyhlásenia o podpore v interoperabilnom formáte, akým je napríklad rozšíriteľný značkový jazyk XML (Extensible Markup Language).

3.3. Vyexportované vyhlásenia o podpore sú označené ako *obmedzená distribúcia* pre príslušný členský štát a ako *osobné údaje*.

3.4. Elektronický prenos vyexportovaných údajov pre členské štáty sa zabezpečí pred odpočúvaním prostredníctvom vhodného šifrovania po celej dĺžke spojenia.