II

(Ikke-lovgivningsmæssige retsakter)

FORORDNINGER

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) Nr. 1179/2011

af 17. november 2011

om fastsættelse af tekniske specifikationer for onlineindsamlingssystemer i henhold til Europa-Parlamentets og Rådets forordning (EU) nr. 211/2011 om borgerinitiativer

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 211/2011 af 16. februar 2011 om borgerinitiativer [1], særlig artikel 6, stk. 5,

efter høring af Den Europæiske Tilsynsførende for Databeskyttelse, og

ud fra følgende betragtninger:

(1) Forordning (EU) nr. 211/2011 fastsætter, at systemer, der anvendes ved onlineindsamling af støttetilkendegivelser, skal opfylde visse sikkerhedskrav og tekniske krav samt godkendes af den kompetente myndighed i den pågældende medlemsstat.

(2) Et onlineindsamlingssystem er i henhold til forordning (EU) nr. 211/2011 et informationssystem bestående af software, hardware, et hostingmiljø, forretningsprocesser og personale, der anvendes til onlineindsamling af støttetilkendegivelser.

(3) Forordning (EU) nr. 211/2011 opstiller de krav, onlineindsamlingssystemer skal opfylde for at blive godkendt, og fastsætter, at Kommissionen bør vedtage tekniske specifikationer til opfyldelse af disse krav.

(4) Top 10 2010-projektet under The Open Web Application Security Project (OWASP) giver et overblik over de største risici for webapplikationssikkerheden og redskaber til at imødegå disse risici; de tekniske specifikationer trækker derfor på de konklusioner, der er draget i forbindelse med dette projekt.

(5) Initiativtagernes anvendelse af tekniske specifikationer bør sikre medlemsstatsgodkendelse af onlineindsamlingssystemerne og bidrage til at sikre iværksættelse af passende tekniske og organisatoriske foranstaltninger, som opfylder de forpligtelser, der er fastsat ved Europa-Parlamentets og Rådets direktiv 95/46/EF [2] om sikkerhed i forbindelse med databehandling — både ved udformning af databehandlingssystemet og ved selve databehandlingen — for at værne om sikkerheden og derved forhindre enhver uautoriseret databehandling og beskytte personoplysninger mod hændelig eller ulovlig tilintetgørelse, hændeligt tab, ændringer, uautoriseret videreformidling eller adgang.

(6) Godkendelsesproceduren bør lettes ved, at initiativtagerne anvender software som Kommissionen stiller til rådighed i henhold til artikel 6, stk. 2, i forordning (EU) nr. 211/2011.

(7) Ved onlineindsamling af støttetilkendegivelser bør initiativtagerne bag borgerinitiativer i deres egenskab af registeransvarlige anvende de tekniske specifikationer, der fastsættes ved denne forordning, for at sikre beskyttelse af de personoplysninger, der behandles. Foretages databehandlingen af en registerfører, skal initiativtagerne sikre, at denne kun handler i overensstemmelse med initiativtagernes instrukser og overholder de tekniske specifikationer, der er fastsat ved denne forordning.

(8) Denne forordning er i overensstemmelse med de grundlæggende rettigheder og de principper, der er fastsat i Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 8, som fastsætter, at enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.

(9) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelse fra det udvalg, der er nedsat ved artikel 20 i forordning (EU) nr. 211/2011 —

[1] EUT L 65 af 11.3.2011, s. 1.

[2] EFT L 281 af 23.11.1995, s. 31.

VEDTAGET DENNE FORORDNING:

Artikel 1

De tekniske specifikationer, der er omhandlet i artikel 6, stk. 5, i forordning (EU) nr. 211/2011, er angivet i bilaget.

Artikel 2

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 17. november 2011.

På Kommissionens vegne
José Manuel BARROSO
Formand

BILAG

1. TEKNISKE SPECIFIKATIONER TIL GENNEMFØRELSE AF ARTIKEL 6, STK. 4, LITRA a), I FORORDNING (EU) Nr. 211/2011

For at forhindre automatiseret indsendelse af en støttetilkendegivelse ved anvendelse af systemet skal underskriverne igennem et passende kontrolforløb, som er i overensstemmelse med almindelig praksis, inden indsendelse af støttetilkendegivelsen. Én mulig kontrolproces, der kan anvendes, er en stærk »captcha«.

2. TEKNISKE SPECIFIKATIONER TIL GENNEMFØRELSE AF ARTIKEL 6, STK. 4, LITRA b), I FORORDNING (EU) Nr. 211/2011

Informationssikringsstandarder

2.1. Initiativtagerne fremlægger dokumentation for, at de opfylder kravene for ISO/IEC 27001-standarden, også selv om de ikke har vedtaget den. De har med henblik herpå:

a) foretaget en fuldstændig risikovurdering, som vedrører systemets anvendelsesområde, aktivitetsmæssige konsekvenser i tilfælde af forskellige informationssikringssvigt, informationssystemets risici og sårbarhed, samt omfatter et risikoanalysedokument, der også angiver modforanstaltninger over for sådanne risici og forholdsregler, der vil blive truffet, hvis der opstår risici, og som endelig opstiller en prioriteret liste over forbedringer

b) fastlagt og gennemført foranstaltninger til imødegåelse af risici med hensyn til beskyttelse af personoplysninger og af familie- og privatlivet samt angivet foranstaltninger, der vil blive truffet, hvis der opstår risici

c) redegjort skriftligt for øvrige risici

d) tilvejebragt organisatoriske redskaber til at modtage feedback om nye trusler og sikkerhedsforbedringer.

2.2. Initiativtagerne skal vælge sikkerhedskontroller, der er baseret på risikoanalysen i punkt 2.1, litra a), blandt følgende standarder:

1) ISO/IEC 27002 eller

2) »Standard of Good Practice« fra Information Security Forum

med henblik på at adressere følgende spørgsmål:

a) risikovurderinger (ISO/IEC 27005 eller en anden specifik og egnet risikovurderingsmetode anbefales)

b) fysisk og miljømæssig sikkerhed

c) personalesikkerhed

d) styring af kommunikation og operationer

e) standardadgangskontrolforanstaltninger — ud over dem, der er fastsat ved denne gennemførelsesforordning

f) indkøb, udvikling og vedligeholdelse af it-systemer

g) håndtering af brud på it-sikkerheden

h) foranstaltninger til at afhjælpe svigt i informationssystemer, der kan resultere i tilintetgørelse eller hændelig tilintetgørelse, ændringer, uautoriseret videreformidling eller adgang til personoplysninger, der behandles

i) overholdelse af regler

j) edb-netværkssikkerhed (ISO/IEC 27033 eller SoGP anbefales).

Anvendelsen af disse standarder kan begrænses til de dele af organisationen, der er relevante for onlineindsamlingssystemet. For eksempel kan personalesikkerheden begrænses til personale, der har fysisk adgang eller netværksadgang til onlineindsamlingssystemet, og den fysiske sikkerhed/den miljømæssige sikkerhed kan begrænses til bygninger, der huser systemet.

Funktionskrav

2.3. Onlineindsamlingssystemet består af en webbaseret applikationsinstans, der er etableret med det formål at indsamle tilkendegivelser af støtte til et enkelt borgerinitiativ.

2.4. Hvis forvaltningen af systemet kræver forskellige roller, etableres der forskellige adgangskontrolniveauer efter princippet om minimering af autorisation.

2.5. De elementer, som offentligheden har adgang til, er klart adskilt fra dem, der anvendes til administrationsformål. Ingen adgangskontrol hindrer adgang til de oplysninger, der er tilgængelige i den offentlige del af systemet, herunder oplysninger om initiativet og den elektroniske støttetilkendegivelsesformular. Det er kun muligt at støtte et initiativ via denne offentlige del.

2.6. Systemet detekterer og forhindrer indsendelse af mere end én støttetilkendegivelse.

Applikationssikkerhedsniveau

2.7. Systemet er på passende vis beskyttet mod kendte svagheder og kendt udnyttelse. Det opfylder derfor bl.a. følgende krav:

2.7.1. Systemet beskytter mod injektionsfejl som f.eks. søgninger med Structured Query Language (SQL), søgninger med Lightweight Directory Access Protocol (LDAP), søgninger med XML Path Language (XPath), Operating System (OS)-kommandoer eller programargumenter. Det er i den forbindelse minimumskrav, at:

a) alt brugerinput valideres

b) validering som et minimum sker via serverens software

c) der ved al brug af tolkningsprogrammer sker en tydelig adskillelse af upålidelige data fra kommandoen eller søgningen. For SQL-søgningers vedkommende betyder det, at der skal anvendes bindevariabler i alle forberedte erklæringer og lagrede procedurer, og at man undgår dynamiske søgninger.

2.7.2. Systemet beskytter mod Cross-Site Scripting (XSS). Det er i den forbindelse minimumskrav, at:

a) det kontrolleres, at alt brugerinput, som sendes tilbage til browseren, er sikkert (ved inputvalidering)

b) alt brugerinput er genstand for escape, inden det inkluderes på outputsiden

c) passende outputkodning sikrer, at denne type input altid behandles som tekst i browseren. Der anvendes ikke aktivt indhold.

2.7.3. Systemet har en effektiv autentiserings- og sessionsstyring, der som et minimum kræver, at:

a) kredentialer altid beskyttes, når de lagres, ved anvendelse af hashing eller kryptering. Risikoen for autentisering ved anvendelse af »pass-the-hash« reduceres

b) kredentialer ikke kan gættes, og at man ikke kan overskrive disse på grund af svage kontoforvaltningsfunktioner (f.eks. kontooprettelse, ændring af password, genfinding af password, svage sessionsidentifikatorer (ID'er))

c) sessions-ID'er og sessionsdata ikke er tilgængelige i Uniform Resource Locator (URL)

d) sessions-ID'er ikke er sårbare over for sessionsfikseringsangreb

e) timeout for sessions-ID'er sikrer, at brugere logger ud

f) sessions-ID'er ikke genanvendes efter veloverstået login

g) password, sessions-ID'er og andre kredentialer kun sendes via Transport Layer Security (TLS)

h) systemets administrationsdel er beskyttet. Hvis den er beskyttet af en enkeltfaktorautentisering, består passwordet af mindst 10 karakterer, herunder mindst et bogstav, et tal og en specialkarakter. Alternativt kan der anvendes tofaktorautentisering. Hvor der kun anvendes enkeltfaktorautentisering, omfatter den en verifikationsmekanisme i to trin for adgang til systemets administrationsdel via internettet, hvor der til enkeltfaktoren føjes et andet autentiseringselement, f.eks. en engangs-passphrase eller en kode via SMS eller en asymmetrisk krypteret tilfældig challengestreng, der dekrypteres under anvendelse af initiativtagerens/administratorens private nøgle, som ikke er kendt af systemet.

2.7.4. Systemet har ikke usikre direkte objektreferencer. Det er i den forbindelse minimumskrav, at:

a) applikationen for direkte referencer til begrænsede ressourcer verificerer, at brugeren har ret til at få adgang til præcis den ønskede ressource

b) hvis referencen er en indirekte reference, er mapping til den direkte reference begrænset til værdier, som er godkendt for den pågældende bruger.

2.7.5. Systemet beskytter mod cross-site request forgery.

2.7.6. Der skal være gennemført passende sikkerhedskonfigurering, som mindst kræver, at:

a) alle softwarekomponenter er up-to-date, herunder OS, web-/applikationsserver, Data Base Management System (DBMS), applikationer og alle kodebiblioteker

b) tjenester, som ikke er nødvendige for OS og web-/applikationsserver, desaktiveres, fjernes eller ikke installeres

c) standardkontopassword ændres eller desaktiveres

d) der etableres fejlhåndtering til at forebygge stack trace og andre fejlmeldinger med for stort informationsindhold

e) sikkerhedsindstillinger i udviklingsrammer og -biblioteker konfigureres i overensstemmelse med god praksis, f.eks. OWASP-retningslinjerne.

2.7.7. Systemet krypterer følgende oplysninger:

a) personoplysninger i elektronisk format krypteres ved lagring eller overførsel til de kompetente myndigheder i medlemsstaterne i henhold til artikel 8, stk. 1, i forordning (EU) nr. 211/2011, og forvaltning og back up af nøgler sker separat

b) stærke standardalgoritmer og stærke nøgler anvendes i overensstemmelse med internationale standarder. Nøgleforvaltning er på plads

c) passwords hashes med en stærk standardalgoritme og velegnet salt

d) alle nøgler og password er beskyttet mod uautoriseret adgang.

2.7.8. Systemet begrænser URL-adgang baseret på brugeradgangsniveauer og -tilladelser. Det er i den forbindelse minimumskrav, at:

a) eksterne sikkerhedsmekanismer skal have en passende konfigurering for hver side, hvis de anvendes til autentiserings- og autorisationskontrol for sideadgang

b) eventuelt anvendt kodeniveaubeskyttelse skal være på plads for alle de nødvendige sider.

2.7.9. Systemet anvender tilstrækkelig Transport Layer Protection. Til det formål skal alle de følgende foranstaltninger — eller tilsvarende stærke foranstaltninger — være på plads:

a) systemet kræver anvendelse af den seneste version af Hypertext Transfer Protocol Secure (HTTPS) for adgang til enhver følsom ressource under anvendelse af certifikater, der er gyldige, ikke-udløbne, ikke-tilbagekaldte, og som matcher alle de domæner, der anvendes af sitet

b) systemet angiver »sikker«-flag på alle følsomme cookies

c) serveren konfigurerer TLS-protokollen, således, at den kun støtter krypteringsalgoritmer i overensstemmelse med god praksis. Brugerne informeres om, at deres browser skal være forberedt til TLS-støtte.

2.7.10. Systemet beskytter mod ikke-valideret redirect og forward.

Databasesikkerhed og dataintegritet

2.8. Hvor onlineindsamlingssystemer, der anvendes til forskellige borgerinitiativer, deler hardware og operativsystemressourcer, deler de ikke data, heller ikke adgangs- eller krypteringskredentialer. Dette afspejles også i risikovurderingen og de gennemførte modforanstaltninger.

2.9. Risikoen for, at der foretages databaseautentisering ved anvendelse af »pass-the-hash« mindskes.

2.10. De oplysninger, der opgives af underskriverne, er kun tilgængelige for databaseadministratoren/initiativtageren.

2.11. Administrative kredentialer, personoplysninger hidrørende fra underskrivere og tilhørende backup sikres via stærke krypteringsalgoritmer som angivet i punkt 2.7.7, litra b). Systemet kan imidlertid foretage ikke-krypteret lagring af den medlemsstat, hvor støttetilkendegivelsen optælles, datoen for tilkendegivelse af støtte og det sprog, underskriveren anvendte ved udfyldelsen af støttetilkendegivelsesformularen.

2.12. Underskriverne har kun adgang til oplysninger, der er afgivet i løbet af den session, hvor de udfylder støttetilkendegivelsesformularen. Når støttetilkendegivelsen indsendes, afsluttes den ovennævnte session, hvorefter de opgivne oplysninger ikke længere er tilgængelige.

2.13. Underskrivernes personoplysninger er kun tilgængelige i systemet — herunder backup — i krypteret format. Med henblik på konsultering af oplysninger eller attestering fra de nationale myndigheders side i henhold til artikel 8 i forordning (EU) nr. 211/2011 kan initiativtagerne eksportere de krypterede oplysninger som angivet i punkt 2.7.7, litra a).

2.14. De oplysninger, der indføres i støttetilkendegivelsesformularen, har en atomisk persistens. Dvs. at når brugeren har indført alle de krævede oplysninger i støttetilkendegivelsesformularen og validerer sin beslutning om at støtte initiativet, så overfører systemet enten alle formularoplysninger til databasen eller gemmer i tilfælde af fejl ingen oplysninger. Systemet informerer brugeren om, hvorvidt dennes anmodning er registreret eller ej.

2.15. Det anvendte DBMS er up-to-date og patcher løbende huller, der detekteres.

2.16. Alle systemets aktivitetslogge er på plads. Systemet sikrer, at revisionslogge, der registrerer undtagelser og andre sikkerhedsrelevante begivenheder som angivet nedenfor, kan genereres og føres, indtil oplysningerne er destrueret i henhold til artikel 12, stk. 3 eller 5, i forordning (EU) nr. 211/2011. Loggene er beskyttet tilstrækkeligt, f.eks. ved lagring på krypterede medier. Initiativtagerne/administratorerne tjekker regelmæssigt loggene for mistænkelig aktivitet. Loggene indeholder som et minimum:

a) datoer og klokkeslæt for initiativtagernes/administratorernes log-on og log-off

b) gennemført backup

c) alle ændringer og opdateringer, der foretages af databaseadministratoren.

Infrastruktursikkerhed — fysisk placering, netværksinfrastruktur og servermiljø

2.17. *Fysisk sikkerhed*

Uanset den anvendte form for hosting skal applikationens hostingmaskine være tilstrækkeligt beskyttet, hvilket omfatter:

a) adgangskontrol og revisionslog for hostingområde

b) fysisk beskyttelse af backupdata mod tyveri eller hændelig fejlplacering

c) at værtsserveren for applikationen er installeret i sikret rack.

2.18. *Netværkssikkerhed*

2.18.1. Systemets host er en internetorienteret server, som er installeret i en demilitariseret zone og beskyttet af en firewall.

2.18.2. Når relevante opdateringer og patchninger af firewallproduktet bliver offentlige, skal de hurtigt installeres.

2.18.3. Al indgående og udgående servertrafik (i tilknytning til onlineindsamlingssystemet) kontrolleres via firewallreglerne og logges. Gennem firewallreglerne afvises al trafik, der ikke er nødvendig for sikker anvendelse og styring af systemet.

2.18.4. Onlineindsamlingssystemet kræver et tilstrækkeligt beskyttet produktionsnetværksegment, der er adskilt fra segmenter, der fungerer som host for ikke-produktionssystemer som f.eks. udviklings- eller testmiljøer.

2.18.5. Local Area Network (LAN)-sikkerhedsforanstaltninger som de nedenstående er på plads:

a) Layer 2 (L2)-adgangsliste/port switch-sikring

b) ubenyttede switchporte desaktiveres

c) den demilitariserede zone findes på et særligt Virtual Local Area Network (VLAN)/LAN

d) L2-trunkering skal ikke være mulig for unødvendige porte.

2.19. *Sikkerhed for OS og web-/applikationserver*

2.19.1. Der skal forefindes en passende sikkerhedskonfiguration, som inkluderer de elementer, der er angivet i punkt 2.7.6.

2.19.2. Applikationerne anvender størst mulig minimering af autorisation.

2.19.3. Administratoradgang til forvaltningsinterface for onlineindsamlingssystemet med en kort sessions-time-out (højst 15 minutter).

2.19.4. Når relevante opdateringer og patchning af OS, applikationskøretider, applikationer, der kører på serverne, eller anti-malware er blevet offentlige, så installeres sådanne opdateringer eller patchninger med det samme.

2.19.5. Risikoen for, at der foretages systemautentisering ved anvendelse af »pass-the-hash« mindskes.

2.20. *Initiativtagernes sikkerhedsforanstaltninger for kunder*

Af hensyn til end-to-end-sikkerheden træffer initiativtagerne de nødvendige foranstaltninger til at sikre deres kundeapplikationer/-anordninger, som de anvender til at forvalte og få adgang til onlineindsamlingssystemet, f.eks.:

2.20.1. Brugerne gennemfører ikke-vedligeholdelsesopgaver (i forbindelse med f.eks. kontorudstyr) med størst mulig minimering af autorisation.

2.20.2. Når relevante opdateringer og udbedringer af OS, enhver installeret applikation eller anti-malware bliver offentlige, skal disse opdateringer og patchninger installeres med det samme.

3. TEKNISKE SPECIFIKATIONER TIL GENNEMFØRELSE AF ARTIKEL 6, STK. 4, LITRA c), I FORORDNING (EU) Nr. 211/2011

3.1. Systemet giver mulighed for, at der for hver enkelt medlemsstat kan udskrives en rapport om initiativet og personoplysninger for underskriverne, som verificeres af den kompetente myndighed i den pågældende medlemsstat.

3.2. Eksport af underskrivernes støttetilkendegivelser er mulig i det format, der er angivet i bilag III til forordning (EU) nr. 211/2011. Det kan også være muligt med systemet at eksportere støttetilkendegivelserne i et interoperabelt format som f.eks. Extensible Markup Language (XML).

3.3. De eksporterede støttetilkendegivelser mærkes med *begrænset distribution* i den pågældende medlemsstat og betegnes som *personoplysninger*.

3.4. Den elektroniske transmission af eksporterede oplysninger til medlemsstaterne sikres mod dataopfangning ved egnet end-to-end-kryptering.