II

(Icke-lagstiftningsakter)

FÖRORDNINGAR

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) nr 1179/2011

av den 17 november 2011

om tekniska specifikationer för system för insamling via internet i enlighet med Europaparlamentets och rådets förordning (EU) nr 211/2011 om medborgarinitiativet

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) nr 211/2011 av den 16 februari 2011 om medborgarinitiativet ([1]), särskilt artikel 6.5,

efter att ha hört Europeiska datatillsynsmannen, och

av följande skäl:

(1) Enligt förordning (EU) nr 211/2011 ska behörig myndighet i den aktuella medlemsstaten intyga att de system som används för insamling av stödförklaringar via internet uppfyller vissa krav beträffande säkerhetsfunktioner och tekniska lösningar.

(2) Ett system för insamling via internet i den mening som avses i förordning (EU) nr 211/2011 är ett informationssystem bestående av programvara, hårdvara, värdmiljö, affärsprocesser och personal för att fullfölja insamlingen av stödförklaringar via internet.

(3) I förordning (EU) nr 211/2011 anges vilka krav som insamlingssystemen måste uppfylla för att få intyg från behörig myndighet. Det anges också att kommissionen bör fastställa tekniska specifikationer för att uppfylla dessa krav.

(4) OWASP:s (Open Web Application Security Project) topplista för 2010 ger en överblick över de största säkerhetsriskerna kring webbaserade tillämpningsprogram samt verktyg för att hantera dessa risker. De tekniska specifikationerna utgår därför från resultatet av detta projekt.

(5) Organisatörerna bör vid införandet av de tekniska specifikationerna se till att medlemsstaternas myndigheter utfärdar intyg för insamlingssystemen och bidrar till det faktiska genomförandet av de tekniska och organisatoriska åtgärder som krävs för att uppfylla skyldigheterna enligt Europaparlamentets och rådets direktiv 95/46/EG ([2]) beträffande säkerheten i samband med behandlingen. Skyldigheterna gäller både vid konstruktionen av systemet och i samband med själva databehandlingen och handlar om att upprätthålla säkerheten, det vill säga förhindra all otillåten behandling av och skydda personuppgifter mot oavsiktlig eller olaglig förstöring eller oavsiktlig utplåning, ändring, otillåtet utlämnande eller otillåten åtkomst.

(6) Intygandeförfarandet bör underlättas av att organisatörerna använder den programvara som kommissionen tillhandahåller och som omnämns i artikel 6.2 i förordning (EU) nr 211/2011.

(7) I egenskap av registeransvariga för insamlingen av stödförklaringar via internet bör medborgarinitiativens organisatörer införa de tekniska specifikationer som anges i denna förordning för att garantera skyddet av de personuppgifter som behandlas. Om uppgifterna behandlas av en registerförare bör organisatörerna se till att denna enbart agerar på uppdrag av organisatörerna och inför de tekniska specifikationer som fastställs i denna förordning.

(8) Hänsyn tas i denna förordning till grundläggande rättigheter och de principer som fastställs i Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artikel 8, om vars och ens rätt till skydd av de personuppgifter som rör honom eller henne.

(9) De åtgärder som fastställs i denna förordning är förenliga med yttrandet från den kommitté som tillsatts i enlighet med artikel 20 i förordning (EU) nr 211/2011.

([1]) EUT L 65, 11.3.2011, s. 1.

([2]) EGT L 281, 23.11.1995, s. 31.

HÄRIGENOM FÖRESKRIVS FÖLJANDE:

Artikel 1

De tekniska specifikationer som anges i artikel 6.5 i förordning (EU) nr 211/2011 anges i bilagan.

Artikel 2

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 17 november 2011.

På kommissionens vägnar
José Manuel BARROSO
Ordförande

BILAGA

1. TEKNISKA SPECIFIKATIONER FÖR GENOMFÖRANDET AV ARTIKEL 6.4 a I FÖRORDNING (EU) nr 211/2011

För att förhindra att stödförklaringar lämnas in automatiskt via systemet, ska undertecknarna på lämpligt sätt kontrolleras i överensstämmelse med gällande praxis innan de lämnar in en stödförklaring. Ett sätt att kontrollera inlämningen är att använda starka ”captcher”.

2. TEKNISKA SPECIFIKATIONER FÖR GENOMFÖRANDET AV ARTIKEL 6.4 b I FÖRORDNING (EU) nr 211/2011

Standard för informationssäkerhet

2.1 Organisatörer ska uppvisa dokumentation som styrker att de uppfyller kraven enligt standard ISO/IEC 27001. De ska därmed ha gjort följande:

a) Genomfört en heltäckande riskbedömning där systemets omfattning definieras, de affärsmässiga konsekvenserna av brister i informationssäkerheten blir belysta, en lista tagits fram över risker och sårbara punkter i informationssystemet liksom en riskanalys med förteckning över motåtgärder för att undvika sådana risker samt lösningar som kan användas vid uppkomna risker. Slutligen ska en prioriteringslista över förbättringar ha utarbetats.

b) Konstruerat och vidtagit åtgärder för att hantera risker kring skyddet av personuppgifter och familjeliv och privatliv samt åtgärder. De ska också ha tagit fram åtgärder som ska vidtas om risken uppstår.

c) Skriftligen definierat övriga risker.

d) Tillhandahållit organisatoriska resurser för att kunna ta emot återkoppling beträffande nya hot och säkerhetsförbättringar.

2.2 Organisatörer ska med utgångspunkt i den riskanalys som anges i punkt 2.1. a) välja säkerhetskontroller enligt följande standarder:

1. ISO/IEC 27002 eller

2. ”Standard of Good Practice” från Information Security Forum

för att lösa följande uppgifter:

a) Riskbedömningar (ISO/IEC 27005 eller annan lämplig riskbedömningsmetod rekommenderas).

b) Fysisk säkerhet och säkerhet i IT-miljön.

c) Personalsäkerhet.

d) Ledning för kommunikation och drift.

e) Standardiserade åtkomstkontroller, utöver dem som anges i denna EN genomförandeförordning.

f) Förvärv, utveckling och drift av informationssystem.

g) Hantering av informationssäkerhetsrelaterade händelser.

h) Åtgärder för att avhjälpa och avgränsa intrång i informationssystem som kan leda till att personuppgifter som hanteras förstörs eller oavsiktligt utplånas, ändras, lämnas ut otillåtet eller beviljas otillåten åtkomst.

i) Överensstämmelse.

j) Datanätsäkerhet (ISO/IEC 27033 eller SoGP rekommenderas).

Standarderna behöver bara tillämpas på de delar av organisationen som berörs av insamlingen via internet. Personalsäkerheten kan till exempel begränsas till att endast gälla de anställda som har fysisk tillgång eller tillgång via nätverk till insamlingssystemet på internet; fysisk säkerhet/IT-miljö kan begränsas till de byggnader där systemet är inhyst.

Krav på funktion

2.3 Insamlingssystemet på internet består av ett webbaserat tillämpningsprogram som läggs ut för att samla in stödförklaringar till ett medborgarinitiativ.

2.4 Om det krävs olika roller för att hantera systemet ska olika nivåer av åtkomstkontroller införas enligt principen begränsad behörighet.

2.5 De funktioner som kan nås av allmänheten ska vara tydligt åtskilda från de funktioner som är avsedda för administration. Åtkomst till information i systemets offentliga avsnitt ska inte kontrolleras, det vill säga information om initiativet och stödförklaringsblanketten. Ett medborgarinitiativ ska bara kunna undertecknas via detta offentliga utrymme.

2.6 Systemet ska spåra och förhindra att kopior av stödförklaringar lämnas in.

Tillämpningsprogrammets säkerhet

2.7 Systemet ska på lämpligt sätt vara skyddat mot kända brister och angrepp. Det ska därför uppfylla bland annat följande krav:

2.7.1 Systemet ska ha skydd mot brister vid intrång som SQL-anrop (Structured Query Language queries), LDAP-anrop (Lightweight Directory Access Protocol queries), Xpath-anrop (XML Path Language queries), operativsystemkommandon eller programvariabler (argument). Det krävs därför att systemet uppfyller minst följande krav:

a) All inmatning från användare ska kontrolleras.

b) Kontroller ska åtminstone göras genom serverbaserad logik.

c) All användning av tolkar ska vara tydligt åtskild från ej tillförlitliga uppgifter från kommandon eller anrop. Vid SQL-anrop innebär det att bindningsvariabler ska användas i alla förberedda satser och lagrade processer, och dynamiska frågor undvikas.

2.7.2 Systemet ska ha skydd mot XSS (Cross-Site Scripting). Det ska därför uppfylla minst följande krav:

a) All indata från användarna som skickas tillbaka till webbläsaren ska kontrolleras så att den är säker (via indatakontroll).

b) All indata från användarna ska avlägsnas korrekt innan den placeras på en sida med utdata.

c) Korrekt kodning av utdata ska säkerställa att sådana indata alltid behandlas som text i webbläsaren. Inget aktivt innehåll ska användas.

2.7.3 Systemet ska ha kraftig autentiserings- och sessionsstyrning. Det ska därför uppfylla minst följande krav:

a) Lagrade behörighetsuppgifter ska alltid skyddas med hjälp av hashvärden eller kryptering. Risken för att någon kan bli godkänd genom att gå förbi hashvärdet (”pass-the-hash”) ska begränsas.

b) Behörighetsuppgifter ska inte kunna gissas eller skrivas om på grund av brister i kontohanteringen (till exempel genom att skapa konto, byta eller återanvända lösenord eller på grund av svagt sessions-id).

c) Sessions-id och sessionsdata ska inte vara synliga i webbadressen (URL).

d) Session-id ska inte kunna påverkas genom angrepp mot dess inställningar.

e) Det ska finnas en tidsgräns för sessions-id som gör att användare måste logga ut.

f) Sessions-id ska inte roteras efter avslutad inloggning.

g) Lösenord, sessions-id och andra behörighetsuppgifter ska enbart skickas via TLS-protokoll.

h) Systemets administrativa del ska vara skyddad. Om den är skyddad med enfaktorsautentisering ska lösenordet bestå av minst tio tecken, varav minst en bokstav, en siffra och ett specialtecken. Tvåfaktorsautentisering kan också användas. När enbart enfaktorsautentisering används ska den kontrollera åtkomst till systemets administrativa del via internet i två steg. Den ensamma faktorn ska då förstärkas med annan autentisering, till exempel engångslösenord/kod via sms eller asymmetriskt krypterade slumpmässigt styrda bekräftelsesträngar som avkrypteras med hjälp av organisatörens/administratörens privata lösenord som är okänt för systemet.

2.7.4 Systemet ska inte ha några oskyddade direkta objekthänvisningar. Det ska därför uppfylla minst följande krav:

a) Vid direkta hänvisningar till resurser som kräver behörighet ska tillämpningsprogrammet kontrollera att användaren har tillåtelse att komma åt just den resurs som begärs.

b) Om hänvisningen är indirekt ska mappning till den direkta hänvisningen bara gälla för de värden som den aktuella användaren är godkänd för.

2.7.5 Systemet ska ha skydd mot bedrägerier med förfalskade anrop från bedrägliga webbplatser (CSRF).

2.7.6 Systemet ska ha korrekta säkerhetsinställningar. Det ska därför uppfylla minst följande krav:

a) All programvara ska vara uppdaterad, inklusive operativsystem, server för webb/tillämpningsprogram, databashanterare, tillämpningsprogram och kodbibliotek.

b) Tjänster som inte är nödvändiga för operativsystem eller server för webb/tillämpningsprogram ska avaktiveras, avlägsnas eller inte installeras.

c) Standardinställda kontolösenord ska ändras eller avaktiveras.

d) Felhanteringsmetod ska skapas för att förhindra stackspårning eller att andra överflödiga felmeddelanden läcker ut.

e) Säkerhetsinställningarna i ramverk för utveckling och bibliotek ska följa bästa praxis, exempelvis riktlinjerna från OWASP.

2.7.7 Systemet ska kryptera uppgifter enligt följande:

a) Personuppgifter i elektroniskt format ska krypteras när de lagras eller överförs till behöriga myndigheter i medlemsstaterna i enlighet med artikel 8.1 i förordning (EU) nr 211/2011. Krypteringsnycklar ska hanteras och säkerhetskopieras separat.

b) Kraftiga standardalgoritmer och starka krypteringsnycklar ska användas enligt internationell standard. Det ska finnas ledningssystem för krypteringsnycklarna.

c) Lösenord ska förses med hashvärde med hjälp av en stark standardalgoritm; lämpligt saltvärde ska användas.

d) Alla krypteringsnycklar och lösenord ska skyddas från otillåten åtkomst.

2.7.8 Systemet ska begränsa URL-åtkomst på grundval av användarens behörighetsnivå och tillstånd. Det ska därför uppfylla minst följande krav:

a) Om externa säkerhetsmekanismer används för autentiserings- och behörighetskontroller vid åtkomst till webbsida måste de vara korrekt inställda för varje sida.

b) Om skyddet ligger på kodnivå måste det finnas skydd för varje anropad sida.

2.7.9 Systemet ska ha tillräckligt skydd via TLS. Det krävs därför att samtliga följande åtgärder, eller åtgärder som är minst lika kraftfulla, har vidtagits:

a) Systemet ska ha den senaste HTTPS-versionen för åtkomst till alla känsliga resurser med hjälp av certifikat som är giltiga, inte har löpt ut eller återkallats och som passar för alla domäner som används på webbplatsen.

b) Systemet ska markera alla känsliga cookies med ”säker flagga”.

c) Serverns TLS-inställningar ska tillåta att endast krypterade algoritmer stöds i enlighet med bästa praxis. Användarna ska informeras om att de måste möjliggöra TLS i sin webbläsare.

2.7.10 Systemet ska ha skydd mot ogiltiga omdirigeringar och vidarebefordringar.

Databassäkerhet och dataskydd

2.8 Om ett system för insamling via internet används för olika medborgarinitiativ med samma hårdvara och operativsystem ska varken uppgifter eller behörighetsuppgifter för åtkomst/kryptering användas gemensamt. Detta ska också återspeglas i riskbedömningen och i de motåtgärder som vidtas.

2.9 Risken för att någon blir autentiserad på databasen genom att kringgå hashvärdet ska förhindras.

2.10 Uppgifter som lämnas av undertecknarna ska bara vara åtkomliga för databasens administratör/organisatör.

2.11 Administrativa behörighetsuppgifter, personuppgifter insamlade från undertecknare och säkerhetskopior av dem ska skyddas via kraftiga krypteringsalgoritmer i enlighet med punkt 2.7.7 b. Uppgifter om datum då stödförklaringen inlämnats och vilket språk undertecknaren använt på blanketten kan dock lagras i systemet utan kryptering i den medlemsstat där stödförklaringarna ska räknas.

2.12 Undertecknarna ska bara ha åtkomst till de uppgifter som lämnats under den session då de fyller i stödförklaringsblanketten. När blanketten väl är inlämnad stängs sessionen och de uppgifter som lämnats är inte längre tillgängliga.

2.13 Undertecknarnas personuppgifter ska bara vara tillgängliga i systemet, inklusive i säkerhetskopior, i krypterad form. Organisatörerna kan dock exportera de krypterade uppgifterna i enlighet med punkt 2.7.7 a för de nationella myndigheternas uppgiftskontroller och intygande i enlighet med artikel 8 i förordning (EU) nr 211/2011.

2.14 De uppgifter som läggs i stödförklaringsblankett ska ha odelbar varaktighet. Det innebär att när användaren väl har lagt in alla nödvändiga uppgifter i blanketten och godkänt sitt beslut att stödja initiativet ska systemet antingen överföra samtliga uppgifter till databasen eller, om fel uppstår, inte spara några uppgifter alls. Systemet ska meddela användaren huruvida hans/hennes kommando har genomförts eller inte.

2.15 Den databashanterare som används ska vara uppdaterad och fortlöpande korrigerad i fråga om nyupptäckta risker.

2.16 Alla aktivitetsloggar för systemet ska vara installerade. Systemet ska garantera att revisionsloggar med registrerade undantag och andra säkerhetsrelaterade händelser som anges nedan kan tas fram och sparas tills uppgifterna har förstörts i enlighet med artikel 12.3 eller 12.5 i förordning (EU) nr 211/2011. Loggarna ska vara adekvat skyddade, till exempel lagras på krypterade medier. Organisatörer/administratörer ska regelbundet gå igenom loggarna för att söka misstänkta händelser. Loggarna ska minst omfatta följande:

a) Datum och tidpunkt för organisatörers/administratörer in- respektive utloggning.

b) Utförd säkerhetskopiering.

c) Alla förändringar och uppdateringar gjorda av databasens administratör.

Infrastruktursäkerhet – fysisk plats, nätverksstruktur och servermiljö

2.17 *Fysisk säkerhet*

Oavsett hur systemet är inhyst ska den utrustning som används för tillämpningsprogrammet vara lämpligt skyddad enligt följande:

a) Åtkomsten till och logg över det område där utrustningen förvaras ska kontrolleras.

b) Säkerhetskopior ska vara fysiskt skyddade mot stöld eller oavsiktlig förlust.

c) Den server som används för tillämpningsprogrammet ska installeras i en skyddad infattning.

2.18 *Nätverkssäkerhet*

2.18.1 Systemet ska ligga på en server ansluten till internet och installerad i en demilitariserad zon med skydd av brandvägg.

2.18.2 När ny information offentliggörs om relevanta uppdateringar och korrigeringar av brandväggen ska sådana uppdateringar och korrigeringar installeras utan dröjsmål.

2.18.3 All ingående och utgående trafik till/från servern (avsedd för insamlingssystemet på internet) ska granskas enligt brandväggsreglerna och registreras. Brandväggsreglerna ska innebära att all trafik stoppas som inte behövs för säker användning och styrning av systemet.

2.18.4 Insamlingssystemet på internet ska vara inhyst på ett lämpligt skyddat segment av ett aktivt nätverkssegment som är avskilt från segment som används av andra system, till exempel utveckling eller testmiljöer.

2.18.5 Säkerhetsåtgärder för det lokala nätverket (LAN) ska vara vidtagna, till exempel:

a) Åtkomstlista (L2)/säker switch ska användas.

b) Portar i switchen som inte används ska avaktiveras.

c) Den demilitariserade zonen ska ligga på ett särskilt virtuellt lokalt nätverk (VLAN)/LAN.

d) Ingen L2-överföring ska vara aktiverad på outnyttjade portar.

2.19 *Skydd av operativsystem och server för webb/tillämpningsprogram*

2.19.1 Korrekta säkerhetsinställningar ska finnas och omfatta de faktorer som anges i punkt 2.7.6.

2.19.2 Tillämpningsprogram ska köras med lägsta möjliga behörighet.

2.19.3 Administratörens åtkomst till insamlingssystemets hanterargränssnitt ska ha kort förinställd sessionstid (högst 15 minuter).

2.19.4 När relevanta uppdateringar och korrigeringar av operativsystemet, tillämpningsprogrammets exekvering, körning av tillämpningsprogram på servrar eller virusprogram har offentliggjorts ska sådana uppdateringar och korrigeringar installeras utan dröjsmål.

2.19.5 Risken för att någon får behörighet till systemet genom att kringgå hashvärdet ska begränsas.

2.20 *Organisatörens klientsäkerhet*

För att uppnå säkerhet i alla led ska organisatörerna vidta nödvändiga åtgärder för att säkra den klienttillämpning/anordning de använder för att hantera och nå insamlingssystemet, till exempel följande:

2.20.1 Användare ska utföra uppgifter som inte rör underhållet (till exempel kontorsadministration) med lägsta möjliga behörighetsnivå för uppgiftens genomförande.

2.20.2 När relevanta uppdateringar och korrigeringar av operativsystemet, alla installerade tillämpningsprogram och virusprogram har offentliggjorts ska sådana uppdateringar och korrigeringar installeras utan dröjsmål.

3. TEKNISKA SPECIFIKATIONER FÖR GENOMFÖRANDET AV ARTIKEL 6.4 c I FÖRORDNING (EU) nr 211/2011

3.1 Systemet ska ge möjlighet att för varje enskild medlemsstat ta fram en rapport med förteckning över medborgarinitiativet och undertecknarnas personuppgifter, under förutsättning att de kontrolleras av behörig myndighet i samma medlemsstat.

3.2 Undertecknarnas stödförklaringar ska kunna exporteras i det format som anges i bilaga III till förordning nr 211/2011. Systemet kan också göra det möjligt att exportera stödförklaringarna i förenligt format, till exempel XML.

3.3 De exporterade stödförklaringarna ska för berörd medlemsstat förses med beteckningen *begränsad spridning* och märkas som *personuppgifter*.

3.4 Elektronisk överföring av exporterade uppgifter till medlemsstaterna ska skyddas mot avlyssning med lämplig kryptering i alla led.