MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Metodický pokyn

k postupu atestačních středisek při posuzování elektronických systémů sběru prohlášení o podpoře evropské občanské iniciativy

Verze 1.0

Praha, 20. 3. 2013

Obsah

1 Shrnutí

1.1 Účel dokumentu

Účel dokumentu	Popsat postup pověřených atestačních středisek při posuzování, zda elektronické systémy sběru naplňují základní požadavky nařízení Evropského parlamentu a Rady (EU) č. 211/2011, kladené na online systém sběru, a dále splňují všechny organizačně-technické specifikace uvedené v příloze prováděcího nařízení Komise (EU) č. 1179/2011.
Závaznost dokumentu	Dokument má doporučující charakter

1.2 Zpracovatelé dokumentu

Organizace	Jméno	Funkce v rámci organizace
Ministerstvo vnitra	Eva Černá	Referent odboru všeobecné správy
	Josef Hruška	Referent odboru veřejné správy a eGovernmentu
	Tomáš Kroupa	Referent odboru veřejné správy a eGovernmentu
	Alois Svoboda	Referent odboru veřejné správy a eGovernmentu
	Radomír Šimek	Referent odboru veřejné správy a eGovernmentu
	Vladimír Weis	Referent odboru veřejné správy a eGovernmentu

1.3 Externí součinnost na dokumentu

Organizace	Jméno	Funkce v rámci organizace
Relsie, spol. s r.o.	Martin Dudek	Ředitel certifikačního orgánu Relsie, s.r.o.
	Jan Dientsbier	Partner

1.4 Historie změn

Číslo verze	Datum verze	Popis změny	Garant	Schválil
1.0	20.3.2013	Základní verze dokumentu	Odbor veřejné správy a eGovernmentu	Ředitelka odboru

2 Seznam použitých zdrojů

2.1 Související právní předpisy

Zákon č. 191/2012 Sb., o evropské občanské iniciativě.

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

Nařízení Evropského parlamentu a Rady (EU) č. 211/2011 ze dne 16. února 2011 o občanské iniciativě, dále též jen „nařízení".

Prováděcí nařízení Komise (EU) č. 1179/2011 ze dne 17. listopadu 2011, kterým se stanoví technické specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 211/2011 o občanské iniciativě, dále též jen „prováděcí nařízení".

Směrnice Evropského parlamentu a Rady č. 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

2.2 Související technické normy

ČSN ISO/IEC 27000 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník – česká verze mezinárodní normy ISO/IEC 27000:2009

ČSN ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky – česká verze mezinárodní normy ISO/IEC 27001:2005

ČSN ISO/IEC 27002 Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací – česká verze mezinárodní normy ISO/IEC 17799:2005

ČSN ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací – česká verze mezinárodní normy ISO/IEC 27005:2008

2.3 Terminologický slovník

Atestační středisko – fyzická nebo právnická osoba pověřená k posuzování elektronických systémů sběru (která je současně pověřena k provádění atestací podle zákona č. 365/2000 Sb.).

Důkaz – rozhodující výsledek (zjištění) při uplatnění testovacího scénáře na danou oblast při posuzování souladu elektronického systému sběru s požadavky etalonu (viz dále).

Elektronický systém sběru – elektronický (online) systém sběru prohlášení o podpoře občanské iniciativy, ve smyslu nařízení EU 211/2011. Informační systém, který se skládá ze softwaru, hardwaru, hostitelského prostředí, pracovních postupů a personálu a jehož cílem je provádět elektronický online sběr prohlášení o podpoře.

Etalon – fiktivní ideální elektronický systém sběru splňující úplný soubor nezbytných požadavků na elektronický systém sběru, které jsou stanoveny v čl. 6 a 12 nařízení č. 211/2011 a dále splňující všechny organizačně-technické specifikace uvedené v příloze prováděcího nařízení č. 1179/2011.

Evropská občanská iniciativa – občanská iniciativa dle nařízení EU 211/2011.

Kontrolní listina – matice, do níž jsou shrnuty jednak výsledky analýzy požadavků etalonu na posouzení elektronických systémů sběru (s vazbami na příslušné právní předpisy, s rozdělením na jednotlivé oblasti pro vyhodnocení souladu a způsoby jeho prokazování), jednak navrhované způsoby ověření a vhodné způsoby vyhodnocení souladu. Je přílohou č. 1 tohoto metodického pokynu.

Metrika – soubor veličin, které jsou měřitelné při posuzování elektronického systému sběru.

Organizátoři – organizátoři občanské iniciativy – fyzické osoby tvořící výbor občanů odpovědný za přípravu občanské iniciativy a její předložení Evropské komisi.

Posuzování elektronických systémů sběru (posuzování souladu) – činnost atestačního střediska vykonávaná na základě § 2 až 5 zákona č. 191/2012 Sb. ve smyslu předmětu tohoto metodického pokynu.

Protokol – záznam o výsledcích posouzení souladu elektronického systému sběru s etalonem.

Potvrzení o souladu – Potvrzení o souladu online systému sběru s nařízením Evropského parlamentu a Rady (EU) č. 211/2011 ze dne 16. února 2011 o občanské iniciativě vydané atestačním střediskem, dle přílohy IV nařízení EU 211/2011.

Prohlášení – prohlášení o podpoře občanské iniciativy – formulář, jehož vyplněním daná (podepsaná) osoba vyjadřuje svou podporu (souhlas) občanské iniciativě.

Test – pro účely tohoto dokumentu ověření, respektive přezkoušení chování daného elektronického systému sběru oproti pravidlům nastaveným etalonem. Konkrétním výstupem testu je metrika.

Testovací scénář – konkrétní ověřovacím postup (obsahuje způsob ověření a důkaz) k prokázání souladu elektronického systému sběru s etalonem.

3 Úvod

Zákon č. 191/2012 Sb., o evropské občanské iniciativě, upravuje některé postupy a podmínky pro výkon práva občana členského státu Evropské unie podílet se na demokratickém životě Evropské unie prostřednictvím evropské občanské iniciativy. Organizátoři evropské občanské iniciativy mohou sbírat prohlášení o podpoře občanské iniciativy v listinné nebo v elektronické podobě. Prohlášení sbírají od osob (občanů), které vyplnily do formuláře prohlášení o podpoře své osobní údaje a podepsaly se, čímž vyjádřily svou podporu iniciativě. Podpis není povinný, pokud je formulář zaslán elektronicky bez elektronického podpisu.

Pokud se prohlášení o podpoře sbírají online, musí být elektronický (online) systém sběru prohlášení o podpoře v souladu s nařízením Evropského parlamentu a Rady (EU) č. 211/2011 o občanské iniciativě, a s prováděcím nařízením Komise (EU) č. 1179/2011, kterým se stanoví technické specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 211/2011 o občanské iniciativě. O souladu elektronického systému sběru s uvedenými předpisy (požadavky) vydává pověřená osoba potvrzení o souladu.

Ministerstvo vnitra pověří posuzováním elektronických systémů sběru prohlášení osobu, která je atestačním střediskem podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy.

3.1 Předmět metodického pokynu

Tento metodický pokyn, s odkazem na zákon č. 191/2012 Sb., popisuje postup pověřených atestačních středisek při jejich posuzování, zda elektronické systémy sběru naplňují základní požadavky nařízení č. 211/2011, kladené na online systém sběru v čl. 6 a 12, a dále zda splňují všechny organizačně-technické specifikace uvedené v příloze prováděcího nařízení č. 1179/2011. Je určen pro atestační střediska, která posouzení souladu provádějí.

4 Elektronické systémy sběru

Před zahájením sběru prohlášení v elektronické podobě požádají organizátoři atestační středisko, aby v souladu s požadavky § 4 zákona č. 191/2012 Sb. posoudilo a následně potvrdilo, že elektronický systém sběru, který má být k tomuto účelu používán, je v souladu s čl. 6 a 12 nařízení a vyhovuje návazným organizačně-technickým specifikacím, uvedeným v příloze prováděcího nařízení. Ucelený soubor nezbytných požadavků na elektronický systém sběru (daných uvedenými závaznými akty) vytváří tzv. etalon. Pokud je elektronický systém sběru s takto definovaným etalonem v souladu, vydá za tímto účelem atestační středisko do jednoho měsíce ode dne podání žádosti o posouzení tohoto systému potvrzení podle vzoru uvedeného v příloze IV nařízení.

5 Atestační středisko

5.1 Smluvní vztah s organizátory

Atestační středisko provádí posouzení elektronického systému sběru na základě smlouvy uzavřené s organizátory občanské iniciativy za smluvní cenu. Ke stanovení smluvní ceny organizátoři poskytnou nezbytné informace, zejména k rozsahu dokumentace, způsobu a lokalitách provozování elektronického systému sběru a bližší specifikaci míst ukládání dat.

Podmínky posuzování elektronických systémů sběru (obdoba atestačních podmínek podle zákona č. 365/2000 Sb.) atestační středisko zveřejní na svých internetových stránkách.

Po obdržení poptávky od organizátorů na posouzení elektronického systému sběru atestační středisko organizátorům navrhne uzavření smlouvy. Při schvalování této smlouvy bude rovněž smluvně dohodnut oficiální termín podání žádosti o posouzení, v souladu se zveřejněnými podmínkami.

Datem doručení žádosti o posouzení, začne běžet zákonná lhůta 1 kalendářního měsíce, ve které je atestační středisko povinno provést vlastní posouzení elektronického systému sběru.

5.2 Proces zkoušky (posuzování souladu s etalonem)

Zkoušku tvoří vlastní ověřovací postup (tzv. testovací scénář), v němž se ověřují požadavky etalonu na jednotlivé oblasti elektronického systému sběru k prokázání souladu, a skládá se z následujících kroků:

5.2.1 Zpřístupnění dokumentace elektronického systému sběru atestačnímu středisku

Organizátoři jsou povinni zpřístupnit dokumentaci k elektronickému systému sběru v elektronické podobě a v některém z běžně používaných formátů [pdf, doc(x), xls(x) nebo i dalších, s možností čtení dokumentace pomocí volně šiřitelného programového vybavení]. Dokumentace musí pokrývat všechny požadavky v rozsahu etalonu, který je uveden v kapitole 4.

5.2.2 Posouzení dokumentace

Atestační středisko posoudí zpřístupněnou dokumentaci, zda pokrývá požadavky dané etalonem v celém jeho rozsahu. V případě nalezených neshod ihned zašle jejich seznam a odůvodnění na smluvní kontaktní adresu organizátorů.

Pokud krok posouzení dokumentace proběhne bez nalezení neshod, proces zkoušky pokračuje odstavcem 5.2.4. Údaje o svých zjištěních zaznamenává atestační středisko dle čl. 5.3 písm. h).

5.2.3 Odstranění neshod v dokumentaci

Organizátoři odstraní nalezené neshody a zpřístupní atestačnímu středisku dokumentaci s odstraněnými neshodami. V případě odstranění všech neshod se pokračuje dalším odstavcem 5.2.4.

5.2.4 Posouzení funkčních vlastností a provozních podmínek

Posouzení funkčních vlastností a provozních podmínek na základě zpřístupněné dokumentace a požadavků etalonu se provádí:

a) V místě provozování elektronického systému sběru, pokud je celý nebo zčásti provozován organizátory v jeho prostorách,

b) Na jiném dohodnutém místě, např. v prostorách atestačního střediska, pokud je celý elektronický systém sběru vyvinut a/nebo provozován třetí osobou (například pronájmem provozních kapacit pro systém elektronického systému sběru v datacentru, kompletními cloudovými službami apod.). I v tomto případě je nezbytné ze strany organizátorů prokázat funkční vlastnosti[1] a tu část provozu (minimálně řízení a dohled nad elektronickým systémem sběru), která je nezbytně v kompetenci organizátorů.

Údaje o svých zjištěních zaznamenává atestační středisko dle čl. 5.3 písm. h).

Ty části programového vybavení a provozu elektronického systému sběru, které jsou zajištěny třetími stranami jako služby, musí být dokladovány příslušnými SLA (Service Level Agreement) smlouvami, které zaručují u těchto služeb odpovídající požadavky právních předpisů s tím, že třetí strany berou za ně plnou smluvní odpovědnost. Tím však není dotčena celková právní odpovědnost organizátorů, kteří jsou obecně plně odpovědni Komisi za jimi zvolený elektronický systém sběru, jeho administraci a provoz.

Posouzení funkčních vlastností elektronického systému sběru ze strany atestačního střediska se provádí způsobem testování „black box", tj. po zadání vstupních údajů a jejich zpracování se kontrolují požadované výstupy elektronického systému sběru, včetně chybových hlášení při nesprávných vstupech (např. kontrola na duplicity vstupních záznamů).

Posouzení provozních podmínek atestačním střediskem se provádí auditními procesy a postupy.

V případě že v průběhu tohoto kroku nedojde k nalezení neshod atestačním střediskem, pokračuje atestační středisko dalším krokem. Pokud jsou nalezeny neshody, jsou ze strany atestačního střediska na místě protokolovány a předány organizátorům. Po dohodě s organizátory je stanovena lhůta pro jejich odstranění, s ohledem na možnost opakovaného ověření těchto neshod při dodržení měsíční lhůty pro ukončení posouzení (zkoušky).

5.3 Zaznamenávání údajů v průběhu zkoušky

Atestační středisko zaznamenává údaje o zjištěních, ke kterým dospělo v průběhu zkoušky, do protokolu o provedené zkoušce (dále jen „protokol"). Protokol obsahuje metriku údajů výsledku testů.

Údaje o zjištěních, ke kterým dospělo v průběhu zkoušky, atestační středisko zaznamenává do protokolu ve strukturované formě, a to ke každému posuzovanému hledisku zvlášť; atestační středisko uvede v protokolu klasifikaci

a) splněno, nebo
b) nesplněno.

V protokolu se uvádí

a) identifikační údaje organizátorů,

b) výčet všech dokumentů, které byly k posouzení předloženy, včetně označení jejich verze, počtu stran a data jejich schválení organizátory,

c) název a sídlo atestačního střediska, které provedlo zkoušku,

[1] Pokud je použit kód softwarové aplikace elektronického systému sběru, který je zpřístupněný a spravovaný Komisí, neprovádí se příslušná část posouzení požadovaných funkčních vlastností.

d) jméno nebo jména a příjmení fyzické osoby, která jménem atestačního střediska zkoušku provedla, nebo zaměstnance atestačního střediska, který řídil provedení zkoušky – posouzení,

e) datum zahájení zkoušky a datum jejího ukončení,

f) datum provedení další zkoušky,

g) popis průběhu zkoušky,

h) zjištění, ke kterým atestační středisko dospělo v průběhu zkoušky včetně klasifikace, a to ve formě vyplněné kontrolní listiny.

i) celkový výsledek provedené zkoušky a jeho odůvodnění,

j) jméno nebo jména a příjmení zaměstnance atestačního střediska, který je oprávněn ke schválení protokolu o provedené zkoušce, jeho podpis a datum schválení protokolu.

5.4 Stanovení výsledku zkoušky

Na základě zjištění učiněných při posouzení v průběhu zkoušky atestační středisko stanoví celkový výsledek zkoušky, který charakterizuje zjištění, která byla v průběhu zkoušky učiněna.

Výsledek zkoušky „splňuje" stanoví atestační středisko v případě, že v průběhu posuzování podle čl. 5.2 tohoto pokynu neshledalo žádné nedostatky nebo organizátoři zjištěné nedostatky v průběhu posuzování odstranili.

Výsledek zkoušky „nesplňuje" stanoví atestační středisko v případě, že v průběhu posuzování podle čl. 5.2 tohoto pokynu shledalo nesplnění požadavku, přičemž organizátoři zjištěné nedostatky v průběhu posuzování neodstranili.

V odůvodnění výsledku zkoušky atestační středisko uvede

a) k výsledku zkoušky „**splňuje**" konstatování, že v průběhu posuzování n eshledalo žádné nedostatky nebo organizátoři zjištěné nedostatky odstranili, uvede popis odstraněných nedostatků do případného protokolu, a vydá potvrzení o souladu,

b) k výsledku zkoušky „**nesplňuje**" popis zjištěných nedostatků, a jejich předpokládaný vliv na bezpečné fungování elektronického systému sběru.

Součástí odůvodnění může být protokol s výsledky testů.

6 Vydání potvrzení o souladu

Splňuje-li elektronický systém sběru požadavky podle nařízení, vydá atestační středisko organizátorům do 1 měsíce ode dne podání žádosti o posouzení tohoto systému Potvrzení o souladu online systému sběru s nařízením podle vzoru uvedeného v příloze IV nařízení spolu s odůvodněním (případně protokolem jako neveřejnou částí tohoto Potvrzení o souladu).

Nesplňuje-li elektronický systém sběru požadavky podle nařízení, vyrozumí o tom atestační středisko organizátory do 1 měsíce ode dne podání žádosti o posouzení tohoto systému a předá jim odůvodnění, s uvedením specifikace nesplněných požadavků (případně i příslušný protokol).

7 Přílohy

Kontrolní listina

Je přílohou tohoto metodického pokynu. Na straně jedné jsou uvedeny požadavky etalonu na elektronický systém sběru a na straně druhé atestační středisko zapisuje způsob ověření a důkazy pro jednotlivé oblasti pro vyhodnocení souladu.

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
	Důvody						
odst. 1	Nařízení (EU) č. 211/2011 stanoví, že pokud se prohlášení o podpoře sbírají online, systém použitý k tomuto účelu **musí splňovat určité bezpečnostní a technické požadavky a musí mít potvrzení** od příslušného orgánu dotčeného členského státu.	N/A	N/A	N/A	N/A	N/A	N/A
odst. 2	**Online systém sběru** ve smyslu nařízení (EU) č. 211/2011 **je informační systém**, který se skládá ze **1.softwaru,** **2.hardwaru,** **3.hostitelského prostředí,** **4.pracovních postupů, a** **5.personálu,** a jehož **cílem je provádět online sběr prohlášení o podpoře.**	N/A	N/A	N/A	N/A	N/A	N/A
odst. 3	Nařízení (EU) č. 211/2011 vymezuje požadavky, které musí online systémy sběru splňovat, aby dostaly potvrzení, a stanoví, že Komise by měla přijmout technické specifikace k provedení těchto požadavků.	N/A	N/A	N/A	N/A	N/A	N/A

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
odst. 4	Projekt Top 10 2010 neziskového sdružení OWASP (Open Web Application Security Project) poskytuje přehled nejvážnějších bezpečnostních rizik webových aplikací a nástrojů k řešení těchto rizik; **technické specifikace proto vycházejí ze závěrů tohoto projektu.**	N/A	N/A	N/A	N/A	N/A	N/A
odst. 5	**Provedení** technických specifikací ze strany organizátorů **by mělo zaruči**t, že orgány členských států potvrdí online systémy sběru, a mělo by pomoci zajistit provádění příslušných technických a organizačních opatření potřebných ke splnění **povinností stanovených směrnicí Evropského parlamentu a Rady 95/46/ES (2) o bezpečnosti zpracování** jak v době, kdy se systém zpracovávání navrhuje, tak v době samotného zpracování, aby se udrželo zabezpečení, předešlo se neoprávněnému zpracovávání a aby byla zajištěna ochrana osobních údajů před náhodným nebo nezákonným zničením či náhodnou ztrátou, změnou, neoprávněným odhalením nebo přístupem.	N/A	N/A	N/A	N/A	N/A	N/A
odst. 6	Využívání softwaru poskytnutého Komisí v souladu s článkem 6 odst. 2 nařízení (EU) č. 211/2011 ze strany organizátorů **by mělo usnadnit postup vydávání potvrzen**í.	N/A	N/A	N/A	N/A	N/A	N/A

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
odst. 7	**Organizátoři** občanských iniciativ **by coby správci údajů měli** při online sběru prohlášení o podpoře provádět technické specifikace stanovené v tomto nařízení s cílem zajistit ochranu zpracovávaných osobních údajů. Pokud zpracovávání provádí **zpracovatel**, organizátoři by měli zajistit, aby zpracovatel postupoval jen na základě pokynů organizátorů a aby prováděl technické specifikace stanovené v tomto nařízení.	N/A	N/A	N/A	N/A	N/A	N/A
odst. 8	Toto nařízení dodržuje základní práva a ctí zásady uznávané Listinou základních práv Evropské unie, zejména článek 8 uvedené listiny, který stanoví, že každý má právo na ochranu osobních údajů, které se ho týkají.	N/A	N/A	N/A	N/A	N/A	N/A
odst. 9	Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru zřízeného podle článku 20 nařízení (EU) č. 211/2011,	N/A	N/A	N/A	N/A	N/A	N/A
Článek 1	Technické specifikace uvedené v čl. 6, odst. 5 nařízení (EU) č. 2011/2011, jsou stanoveny v příloze	N/A	N/A	N/A	N/A	N/A	N/A
Článek 2	Toto nařízení vstupuje v platnost dvacátý den po jeho vyhlášení v Úředním věstníku Evropské unie.	N/A	N/A	N/A	N/A	N/A	N/A

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
	Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.	N/A	N/A	N/A	N/A	N/A	N/A
Odst. 1	TECHNICKÉ SPECIFIKACE, JEJICHŽ ÚČELEM JE PROVÁDĚNÍ ČL. **6 ODST. 4 PÍSM**. **a)** NAŘÍZENÍ (EU) č. 211/2011						
	Aby se zabránilo automatizovanému podávání prohlášení o podpoře s využitím systému, absolvuje v souladu se současnou praxí signatář před podáním prohlášení o podpoře řádný proces ověřování. **Jedním z možných způsobů ověřování je využití účinného testu „captcha“.**	T	N/A	N/A	D	N/A	
Odst. 2	TECHNICKÉ SPECIFIKACE, JEJICHŽ ÚČELEM JE PROVÁDĚNÍ **ČL. 6 ODST. 4 PÍSM. b)** NAŘÍZENÍ (EU) č. 211/2011						
	Normy zajištění informací						
Odst. 2.1	**Organizátoři předloží dokumentaci**, která prokazuje, že splňují požadavky normy **ISO/IEC 27001** i bez jejího přijetí. **Za tímto účelem musí:**	D	D	D	D	D	

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
	a) provést úplné hodnocení rizika, v němž -určí rozsah systému, -objasní hospodářské dopady v případě různých porušení zabezpečení informací, -uvedou rizika a slabé stránky informačního systému, -vypracují dokument s analýzou rizika, v němž budou uvedeny také protiopatření na zabránění takovým rizikům a prostředky nápravy, které budou přijaty v případě výskytu rizika, a na závěr -vypracují seznam zdokonalení v upřednostňovaném pořadí;	D	D	D	D	D	
	b) navrhnout a realizovat opatření na řešení rizik souvisejících s ochranou osobních údajů a ochranou rodinného a soukromého života, a opatření, která budou přijata v případě výskytu rizika;	D	D	D	D	D	
	c) v písemné formě pojmenovat další rizika;	D	D	D	D	D	
	d) zajistit organizační prostředky k získání zpětné vazby, co se týče nových hrozeb a vylepšení bezpečnosti.	D	D	D	D	D	
Odst. 2.2	**Organizátoři si zvolí bezpečnostní kontroly** na základě analýzy rizika uvedené v **bodě 2.1 písm. a)** z těchto norem:						

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
	1. ISO/IEC 27002 **nebo**	D	N/A	N/A	N/A	N/A	
	2. „Zásady řádné praxe“ Fóra informační bezpečnosti	D	N/A	N/A	N/A	N/A	
	k řešení těchto věcí:						
	a) hodnocení rizik (doporučuje se ISO/IEC 27005 nebo jiná specifická a vhodná metoda posuzování rizik);	D	D	D	D	D	
	b) fyzická a environmentální bezpečnost;	D	D	D	D	D	
	c) bezpečnost z hlediska lidských zdrojů;	D	D	D	D	D	
	d) komunikace a řízení provozu;	D	D	D	D	D	
	e) standardní opatření ke **kontrole přístupu** jako doplněk k opatřením uvedeným v tomto prováděcím nařízení;	D	D	D	D	D	
	f) akvizice, vývoj a údržba informačních systémů;	D	D	D	D	D	
	g) zvládání incidentů v oblasti bezpečnosti informací;	D	D	D	D	D	
	h) opatření k nápravě a zmírnění narušení informačních systémů, které by vedly ke zničení nebo náhodné ztrátě, změně zpracovávaných osobních údajů, jejich neoprávněnému odhalení nebo přístupu k nim;	D	D	D	D	D	
	i) soulad;	D	D	D	D	D	
	j) bezpečnost počítačové sítě (doporučuje se ISO/IEC 27033 nebo Zásady řádné praxe).	D	D	D	D	D	

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
	Uplatňování těchto norem se může omezovat jen na části organizace, které souvisejí s online systémem sběru. Například zabezpečení lidských zdrojů se může omezovat na personál, který má fyzický nebo síťový přístup k online systému sběru, a fyzická/environmentální bezpečnost se může omezovat na budovy, v nichž se systém nachází.	D	D	D	D	D	
	Funkční požadavky						
Odst. 2.3	Online systém sběru se skládá z webové aplikace vytvořené za účelem sběru prohlášení o podpoře pro jednu občanskou iniciativu.	T/D	N/A	N/A	N/A	N/A	
Odst. 2.4	Jestliže správa systému vyžaduje různé role, vytvoří se různé úrovně přístupu podle zásady nejnižších práv.	T/D	T/D	T/D	D	T/D	
Odst. 2.5	Veřejně přístupné funkce jsou jasně odděleny od funkcí určených pro správu. Kontrola přístupu nebrání čtení informací dostupných ve **veřejné části systému** včetně informací o iniciativě a o elektronickém formuláři prohlášení o podpoře. Připojení se k iniciativě je možné pouze přes veřejně přístupnou část.	T	T+D	T+D	D	T+D	

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
Odst. 2.6	Systém rozeznává podání duplicitního prohlášení o podpoře a zabraňuje mu.	T	T+D	T+D	D	T+D	
	Bezpečnost na úrovni aplikace						
Odst. 2.7	Systém je vhodně zabezpečený, pokud jde o známé slabé stránky a zneužití. Za tímto účelem splňuje **kromě jiného tyto požadavky**:	N/A	N/A	N/A	N/A	N/A	
Odst. 2.7.1	Systém je zajištěn proti injektování kódů (injection flaws), jako jsou: -dotazy v jazyce SQL (Structured Query Language), -dotazy LDAP (Lightweight Directory Access Protocol), -dotazy XPath (XML Path Language), -příkazy operačního systému (OS) nebo argumenty programu. Za tímto účelem je minimálně potřebné, aby:	T+D	N/A	N/A	N/A	N/A	
	a) všechny vstupy uživatelů byly ověřovány;	T	N/A	N/A	D	N/A	
	b) se ověřování provádělo nejméně s pomocí logiky na straně serveru;	T+D	N/A	N/A	N/A	N/A	

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
	c) použití jakýchkoli interpretačních překladačů jasně oddělovalo nedůvěryhodné údaje od příkazu nebo dotazu. V případě volání SQL to znamená použít přiřazené proměnné ve všech připravených prohlášeních a uložených procedurách a vyhnout se dynamickým dotazům.	T+D	N/A	N/A	N/A	N/A	
Odst. 2.7.2	Systém je zajištěn proti XSS (Cross-Site Scripting). Za tímto účelem je minimálně potřebné, aby:						
	a) všechny zadané vstupy uživatelů poslané zpět do prohlížeče byly ověřovány, pokud jde o jejich bezpečnost (prostřednictvím kontroly vstupních parametrů);	T+D	N/A	N/A	N/A	N/A	
	b) všechny vstupy uživatelů byly řádně vráceny do povelové úrovně před jejich začleněním do stránky výstupu;	T+D	N/A	N/A	N/A	N/A	
	c) náležité kódování výstupu zajišťuje, aby prohlížeč takové vstupy vždy považoval za text. Nepoužívá se žádný aktivní obsah.	T+D	N/A	N/A	N/A	N/A	
Odst. 2.7.3	Systém má silné ověřování totožnosti a řízení relací, což minimálně vyžaduje, aby:						

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
	a) identifikační údaje byly při ukládání vždy chráněny pomocí hašování nebo šifrování, aby riziko, že se někdo identifikuje pomocí „pass-the-hash“, bylo minimalizováno;	T+D	N/A	T/D	N/A	N/A	
	b) identifikační údaje se nedaly uhodnout nebo přepsat kvůli slabým funkcím správy účtu (např. vytvoření účtu, změna hesla, získání zapomenutého hesla, slabé identifikátory relace (ID));	T+D	N/A	T/D	N/A	N/A	
	c) identifikátory relace a údaje o relaci se nezobrazovaly v URL (Uniform Resource Locator);	T+D	N/A	T/D	N/A	N/A	
	d) identifikátory relace byly odolné vůči útokům pomocí fixace relací (session fixation);	T+D	N/A	T/D	N/A	N/A	
	e) časový limit identifikátorů relace zajistil odhlášení uživatelů;	T+D	N/A	T/D	N/A	N/A	
	f) identifikátory relace po úspěšném přihlášení nemohly rotovat;	T+D	N/A	T/D	N/A	N/A	
	g) hesla, identifikátory relace a další identifikační údaje se zasílaly jen prostřednictvím TLS (Transport Layer Security);	T+D	N/A	T/D	N/A	N/A	

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
	h) administrativní část systému byla chráněna. Pokud je chráněna jednofaktorovou identifikací, obsahuje heslo minimálně 10 znaků, mezi nimiž je nejméně jedno písmeno, jedna číslice a jeden speciální znak. Případně se může použít dvoufaktorová identifikace. V případě, že se použije pouze jednofaktorová identifikace, zahrnuje tento postup dvoustupňový mechanismus ověřování pro přístup k administrativní části systému přes Internet, v němž se jeden faktor rozšíří o další prostředky identifikace, například o jednorázovou kontrolní větu/kód přes SMS nebo asymetricky zašifrovaný náhodný řetězec (challenge string), který se dešifruje s pomocí osobního klíče organizátora/správce, který systém nezná.	T+D	N/A	T/D	N/A	N/A	
Odst. 2.7.4	**Systém nemá nezajištěné odkazy na přímé objekty. Za tímto účelem je minimálně potřebné, aby:**						
	a) v případě přímých odkazů na omezené zdroje **aplikace ověřila**, zda má uživatel autorizovaný přístup k přesně požadovanému zdroji;	T+D	N/A	N/A	N/A	N/A	
	b) jestliže je odkaz nepřímý, mapování k přímému odkazu bylo omezeno na hodnoty povolené **pro aktuálního uživatele**.	T+D	N/A	N/A	N/A	N/A	

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
Odst. 2.7.5	Systém musí být zajištěn proti zneužití oprávněných dotazů (cross-site request forgery flaw).	T+D	N/A	N/A	N/A	N/A	
Odst. 2.7.6	K dispozici je **náležitá konfigurace zajištění**, což přinejmenším vyžaduje, aby:						
	a) všechny komponenty programového vybavení byly aktuální včetně OS, webového serveru/serveru aplikace, databázového systému (DBMS), aplikací a všech knižnic kódů;	T	N/A	T+D	D	N/A	
	b) nepotřebné funkce OS a webového serveru/serveru aplikace byly vypnuty, vymazány nebo nebyly nainstalovány;	T	N/A	T+D	D	N/A	
	c) implicitně nastavená hesla k účtu se změnila nebo zablokovala;	T	N/A	T+D	D	N/A	
	d) zpracování chyb bylo nastaveno tak, aby zabránilo úniku tzv. stack traces a jiných příliš informativních chybových hlášení;	T	N/A	T+D	D	N/A	
	e) nastavení bezpečnostních parametrů ve vývojových strukturách a knihovnách bylo nakonfigurováno v souladu s osvědčenými postupy, například s pokyny OWASP.	T/D	N/A	T+D	D	N/A	
Odst. 2.7.7	**Systém umožňuje takovéto šifrování údajů:**						

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
	a) Osobní údaje v elektronickém formátu **jsou šifrovány při ukládání** nebo odesílání příslušným orgánům členských států v souladu s čl. 8 odst. 1 nařízení (EU) č. 211/2011, přičemž klíče se spravují a zálohují odděleně.	T+D	N/A	N/A	D	N/A	
	b) Odolné standardní algoritmy a odolné klíče se používají v souladu s mezinárodními normami. K dispozici je správa klíčů.	T	N/A	N/A	D	N/A	
	c) Hesla jsou hašována s pomocí odolného standardního algoritmu a používá se vhodný náhodný řetězec (salt).	T	N/A	N/A	D	N/A	
	d) Všechny klíče a hesla jsou chráněny před neoprávněným přístupem.	T	N/A	N/A	D	N/A	
Odst. 2.7.8	**Systém omezuje přístup URL na základě přístupových úrovní uživatelů a jejich oprávnění.** Za tímto účelem je minimálně potřebné, aby:						
	a) pokud se k zajištění kontroly identifikace a autorizace za účelem přístupu na stránku používají externí bezpečnostní mechanismy, byly náležitě nakonfigurovány pro každou stránku.	T+D	N/A	N/A	D	N/A	

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
	b) Pokud se používá ochrana na základě úrovně kódu, musí být k dispozici pro každou požadovanou stránku.	T+D	N/A	N/A	D	N/A	
Odst. 2.7.9	**Systém využívá dostatečnou ochranu Transport Layer Protection**. Za tímto účelem jsou k dispozici všechna tato opatření nebo minimálně stejně silná opatření:						
	a) Systém vyžaduje nejnovější verzi HTTPS (Hypertext Transfer Protocol Secure) pro přístup ke všem citlivým zdrojům s použitím certifikátů, které jsou platné, neskončila jim platnost, nebyly odvolány a odpovídají všem doménám, které stránka používá.	T	N/A	T/D	D	N/A	
	b) Systém označuje všechny citlivé soubory cookies jako bezpečné.	T+D	N/A	T/D	D	N/A	
	c) Server nakonfiguruje poskytovatele TLS tak, aby podporoval jen šifrovací algoritmy, které odpovídají osvědčeným postupům. Uživatelé jsou informováni, že musí ve svém prohlížeči umožnit podporu TLS.	T	N/A	T/D	D	N/A	
Odst. 2.7.10	Systém poskytuje ochranu proti zrušeným přesměrováním a převodům (forwards).	T	N/A	T/D	D	N/A	
	Bezpečnost databáze a integrita údajů						

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
Odst. 2.8	Pokud online systémy sběru, používané pro různé občanské iniciativy, sdílejí společné zdroje hardwaru a zdroje operačního systému, nesmí sdílet žádné údaje, a to ani přístupové/šifrovací údaje. Promítne se to také v hodnocení rizika a přijatých protiopatření.	T	N/A	T/D	D	N/A	
Odst. 2.9	Riziko, že se někdo identifikuje v databázi pomocí „pass-the-hash“, je minimalizováno.	T	N/A	T/D	D	N/A	
Odst. 2.10	Údaje, které signatáři poskytnou, jsou přístupné jen pro správce databáze/organizátora.	T	N/A	T/D	D	N/A	
Odst. 2.11	Identifikační údaje správce, osobní údaje získané od signatářů a jejich záložní kopie jsou zajištěny s pomocí odolných šifrovacích algoritmů v souladu s bodem 2.7.7 písm. b). V systému však mohou zůstat uloženy tyto nezašifrované údaje: členský stát, jehož se týká prohlášení o podpoře, datum podání prohlášení o podpoře a jazyk, v němž signatář vyplnil prohlášení o podpoře.	T	N/A	T/D	D	N/A	

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
Odst. 2.12	Signatáři mají k poskytnutým údajům přístup pouze v průběhu relace, v níž vyplňují formulář prohlášení o podpoře. Po podání prohlášení o podpoře uvedená relace skončí a poskytnuté údaje už nejsou přístupné.	T	N/A	T/D	D	N/A	
Odst. 2.13	Osobní údaje signatářů jsou v systému, včetně záložních kopií, dostupné pouze v zašifrovaném formátu. Za účelem konzultací o údajích nebo vydání osvědčení ze strany příslušných orgánů v souladu s článkem 8 nařízení (EU) č. 211/2011 mohou organizátoři exportovat šifrované údaje v souladu s bodem 2.7.7 písm. a).	T	N/A	T/D	D	N/A	
Odst. 2.14	Stálost údajů vložených do formuláře prohlášení o podpoře musí být atomická. To znamená, že poté, co uživatel do formuláře prohlášení o podpoře vložil všechny požadované údaje a potvrdil své rozhodnutí podpořit iniciativu, systém buď úspěšně vloží všechny údaje z formuláře do databáze, nebo v případě chyby neuloží žádné údaje. Systém informuje uživatele o úspěchu nebo neúspěchu jeho požadavku.	T	N/A	T/D	D	N/A	
Odst. 2.15	Používaný databázový systém musí být aktuální a musí se neustále vylepšovat o nové prvky.	T	N/A	T/D	D	N/A	

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
Odst. 2.16	**Všechny aktivity systému se protokolují**. Systém zajistí, aby se kontrolní záznamy se zapsanými výjimkami a dalšími níže uvedenými bezpečnostními událostmi mohly vytvořit a uchovávat, dokud tyto údaje nebudou zničeny v souladu s čl. 12 odst. 3 nebo 5 nařízení (EU) č. 211/2011. Záznamy jsou náležitě chráněny, například jejich uložením na zašifrovaných nosičích. Organizátoři/správci pravidelně kontrolují záznamy v souvislosti s podezřelou aktivitou. **Minimální obsah záznamů:**	T+D	N/A	T/D	D	N/A	
	a) datum a čas přihlášení a odhlášení organizátorů/správců;	T	N/A	T/D	D	N/A	
	b) vytvořené záložní kopie;	T	N/A	T/D	D	N/A	
	c) všechny změny a aktualizace správce databáze.	T	N/A	T/D	D	N/A	
	Bezpečnost infrastruktury						
Odst. 2.17	**Fyzická bezpečnost** Bez ohledu na typ použitého hostitelství je technické zařízení, které je hostitelem aplikace, náležitě chráněno, což znamená:						

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
	a) kontrola přístupu k oblasti hostování a kontrolní záznam;	N/A	T/D	T+D	D	T/D	
	b) fyzická ochrana zálohovaných údajů před krádeží nebo náhodným nesprávným umístěním;	N/A	T/D	T+D	D	T/D	
	c) server, který je hostitelem aplikace, je nainstalován v zajištěném rámu.	N/A	T/D	T+D	D	T/D	
Odst. 2.18	**Bezpečnost sítí**						
Odst. 2.18.1	Systém je umístěn na internetovém serveru nainstalovaném v demilitarizované zóně a je chráněn s pomocí systému Firewall.	N/A	T/D	T/D	D	N/A	
Odst. 2.18.2	Po zveřejnění příslušných aktualizací a oprav produktu Firewall jsou tyto neprodleně nainstalovány.	N/A	T/D	T/D	D	N/A	
Odst. 2.18.3	Všechny přenosy na server a ze serveru (určené pro online systém sběru) jsou kontrolovány podle pravidel systému Firewall a protokolují se. Pravidla systému Firewall odmítají všechny přenosy, které nejsou potřebné k bezpečnému používání a správu systému.	N/A	T/D	T/D	D	N/A	
Odst. 2.18.4	Online systém sběru musí být umístěn v řádně zabezpečeném produkčním segmentu sítě, který je oddělen od ostatních segmentů používaných k umístění neprodukčních systémů, například k vývoji nebo testování.	N/A	T/D	T/D	D	N/A	

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
Odst. 2.18.5	Musí být zavedena bezpečnostní opatření pro lokální počítačovou síť (LAN), například:						
	a) seznam přístupů na úrovni 2 (L2)/bezpečnost přepínače rozhraní (port switch);	N/A	T/D	T/D	D	N/A	
	b) nevyužité přepínače rozhraní (switch ports) jsou zablokovány;	N/A	T/D	T/D	D	N/A	
	c) DMZ je umístěna na vyhrazené virtuální lokální počítačové síti (Virtual Local Area Network (VLAN)/LAN);	N/A	T/D	T/D	D	N/A	
	d) seskupení kanálů (trunking) na úrovni L2 se neumožňuje na nepotřebných portech.	N/A	T/D	T/D	D	N/A	
Odst. 2.19	**Bezpečnost OS a webového serveru/serveru aplikace**						
Odst. 2.19.1	Je zajištěna přiměřená konfigurace bezpečnosti včetně prvků uvedených v bodě 2.7.6.	T	N/A	N/A	D	N/A	
Odst. 2.19.2	Aplikace fungují s nejnižší sadou privilegií, která potřebují ke své funkčnosti.	T	N/A	N/A	D	N/A	
Odst. 2.19.3	Přístup správce k rozhraní správy online systému sběru má krátký časový limit (maximálně 15 minut).	T	N/A	N/A	D	N/A	

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
Odst. 2.19.4	Příslušné aktualizace a opravy OS, runtime aplikací, aplikací běžících na serveru nebo aplikací proti škodlivému softwaru, musí být bezodkladně nainstalovány po jejich zveřejnění.	T	N/A	N/A	D	N/A	
Odst. 2.19.5	Riziko, že se někdo identifikuje v systému pomocí „pass-the-hash“, je minimalizováno.	T	N/A	N/A	D	N/A	
Odst. 2.20	**Bezpečnost klienta organizátora** K zajištění bezpečnosti po celé délce spojení přijmou organizátoři nezbytná opatření k tomu, aby zajistili svou klientskou aplikaci/své klientské technické zařízení, které používají k řízení online systému sběru a k přístupu do tohoto systému, **například**:						
Odst. 2.20.1	Uživatelé mohou používat neúdržbové funkce (jako například automatizace administrativy) s nejnižší sadou privilegií potřebných k jejich funkčnosti.	T	N/A	N/A	D	T+D	
Odst. 2.20.2	Bezodkladně po zveřejnění příslušných aktualizací a oprav OS, instalovaných aplikací nebo programů proti malwaru jsou tyto nainstalovány.	T	N/A	N/A	D	T+D	
Odst. 3	TECHNICKÉ SPECIFIKACE, JEJICHŽ ÚČELEM JE PROVÁDĚNÍ ČL. **6 ODST. 4 PÍSM. c)** NAŘÍZENÍ (EU) č. 211/2011						

Etalon ->	**Prováděcí nařízení komise (EU) č. 1179/2011 ze dne 17. 11. 2011, kterým se stanoví specifikace pro online systémy sběru podle nařízení Evropského parlamentu a Rady (EU) č. 2011/2011 o občanské iniciativě.**	Oblasti pro vyhodnocení shody					Symbol **N/A**: není relevantní nebo nevyplňuje se nebo zkouškou se neověřuje Symbol **T**: prokazuje se testem Symbol **D**: prokazuje se z dokumentace Symbol: **T/D**: prokazuje se testem nebo z dokumentace Symbol **T+D**: prokazuje se testem a z dokumentace
Odkaz na ustanovení etalonu	**Text požadavku etalonu**	**1. software**	**2. hardware**	**3. hostitelské prostředí**	**4. pracovní postupy**	**5. personál**	**1. Způsob ověření 2. Jaký důkaz (pro každou oblast)**
Odst. 3.1	Systém poskytuje možnost extrahovat pro jednotlivé členské státy zprávu, v níž bude uvedena iniciativa a osobní údaje signatářů, které podléhají ověření ze strany příslušného orgánu daného členského státu.	T	N/A	N/A	D	N/A	
Odst. 3.2	Prohlášení signatářů o podpoře se mohou exportovat ve formátu přílohy III nařízení č. 211/2011. Systém může kromě toho poskytnout možnost exportovat prohlášení o podpoře v interoperabilním formátu, například v Extensible Markup Language (XML).	T	N/A	N/A	D	N/A	
Odst. 3.3	Exportovaná prohlášení o podpoře jsou označena jako omezená distribuce pro příslušný členský stát a jako osobní údaje.	T	N/A	N/A	D	N/A	
Odst. 3.4	Elektronický přenos exportovaných údajů pro členské státy se zabezpečí před „odposlechem“ s pomocí vhodného zašifrování po celé délce spojení.	T	N/A	N/A	D	N/A	