STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 34980
16 december 2013

Regeling van de Minister van Binnenlandse Zaken en Koninkrijksrelaties van 5 december 2013, nr. 2013-0000744418, houdende regels ter uitvoering van de Verordening (EU) nr. 211/2011 van het Europees Parlement en de Raad van 16 februari 2011 over het burgerinitiatief (PbEU 2011, L 65) (Uitvoeringsregeling verordening Europees burgerinitiatief)

De Minister van Binnenlandse Zaken en Koninkrijksrelaties;

Gelet op artikel 3 van de Uitvoeringswet verordening Europees burgerinitiatief;

Besluit:

Artikel 1

Een aanvraag voor een certificaat als bedoeld in artikel 6, derde lid, van Verordening (EU) nr. 211/2011 van het Europees Parlement en de Raad van 16 februari 2011 over het burgerinitiatief (PbEU 2011, L 65) wordt gedaan door het verstrekken van het volledig ingevulde aanvraagformulier, bedoeld in bijlage 1, bij deze regeling en wordt vergezeld door een volledig ingevulde vragenlijst, bedoeld in bijlage 2, bij deze regeling.

Artikel 2

Deze regeling treedt in werking met ingang van de dag na de datum van uitgifte van de Staatscourant waarin zij wordt geplaatst.

Artikel 3

Deze regeling wordt aangehaald als: Uitvoeringsregeling verordening Europees burgerinitiatief.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk.

BIJLAGE 1

Aanvraagformulier certificering online verzamelsysteem voor Europees Burgerinitiatief

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

1. Gegevens Organisator (en evt. partner(s), zoals hostingpartij of internetprovider)

Organisator: vertegenwoordiger burgercomité		**Partner**	
Naam	:	Naam	:
Straat	:	Straat	:
Postcode	:	Postcode	:
Plaats	:	Plaats	:
Telefoon	:	Telefoon	:
Email	:	Email	:

2. Naam/omschrijving Europees Burgerinitiatief:

☐ is bij de Europese Commissie geregistreerd d.d.

of

☐ heeft bij de Europese Commissie aanvraag tot registratie gedaan d.d.

3. Beschrijving online verzamelsysteem (internetadres/url)

De onder 1. Genoemde Organisator verzoekt de daarvoor aangewezen autoriteit in Nederland om het onder 3. genoemde online verzamelsysteem ten behoeve van het onder 2. genoemde Europese Burgerinitiatief te certificeren conform VERORDENING (EU) Nr. 211/2011.

De Organisator verklaart hierbij:

☐ dat de via het online verzamelsysteem verzamelde gegevens binnen Nederland worden opgeslagen en bewaard (art.6 lid 1)[1]

☐ de door de Commissie ontwikkelde open source software (OCS) versie ongewijzigd te gebruiken.

☐ dat het gebruikte online verzamelsysteem eerder is gecertificeerd d.d.

ten behoeve van Europees Burgerinitiatief (naam, registratienummer)

[1] Wanneer steunbetuigingen online worden verzameld, worden de gegevens die via het onlinesysteem worden verzameld, opgeslagen op het grondgebied van een lidstaat. Het onlinesysteem wordt overeenkomstig de Verordening gecertificeerd in de lidstaat waar de met het onlinesysteem verzamelde gegevens worden opgeslagen.

☐ dat het genoemde online verzamelsysteem voor dit burgerinitiatief niet eerder in een andere lidstaat is afgewezen voor certificering.

☐ dat hij inzicht verschaft in de wijze waarop het IT-systeem is opgebouwd, door middel van een bij dit formulier gevoegd overzicht van het IT-landschap (hardware, software, infrastructuur etc).

☐ dat de vooraf aan te leveren vragenlijst met bijbehorende documentatie juist en volledig ingevuld en bij deze aanvraag bijgevoegd is.

☐ de ten behoeve van de certificering benodigde capaciteit (tijd, medewerkers) voor de vaststelling tijdig en zonder beperkende voorwaarden beschikbaar te hebben en te stellen.

☐ dat aan alle relevante voorwaarden van de Verordening (EU) nr. 211/2011 is voldaan.

☐ dat hij ermee bekend is dat Richtlijn 95/46/EG van toepassing is op de verwerking van persoonsgegevens overeenkomstig deze verordening. Deze Richtlijn gaat over de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. Ook de nationale bepalingen die ter uitvoering van deze Richtlijn zijn vastgesteld, zijn van toepassing. In Nederland betreft dit de Wet bescherming persoonsgegevens.

☐ dit formulier naar waarheid te hebben ingevuld.

Datum:

Naam:

Handtekening:

Dit formulier met de vragenlijst en gevraagde bijlagen svp opsturen aan:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directoraat-Generaal Bestuur en Koninkrijksrelaties
Directie Bestuur, Democratie en Financiën
Afdeling Bestuurlijke Inrichting en Democratie
O.v.v. Aanvraag certificering Europees Burgerinitiatief
Postbus 20011
2500 EA Den Haag

of digitaal aan: europeesburgerinitiatief@minbzk.nl

BIJLAGE 2

Vragenlijst in te vullen door de organisator

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Europees Burgerinitiatief:
Contactpersoon:
Datum ingevuld:

Toelichting bij de vragenlijst

Als u online steunbetuigingen wilt verzamelen voor uw Europees burgerinitiatief, maakt u waarschijnlijk gebruik van een online systeem. Een systeem voor het online verzamelen van steunbetuigingen als bedoeld in Verordening (EU) nr. 211/2011 is een informatiesysteem bestaande uit software, hardware, een hostingomgeving, bedrijfsprocessen en personeel, dat bestemd is voor het online verzamelen van steunbetuigingen. In de Uitvoeringsverordening nr. 1179/2011 van de Europese Commissie staan de technische eisen (specificaties) die gesteld worden aan het onlinesysteem. Als u bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een aanvraag doet tot certificering van uw online verzamelsysteem, moet u bij het aanvraagformulier deze vragenlijst volledig ingevuld en voorzien van de gevraagde documentatie aanleveren.

Hieronder staan in de tabel in de eerste twee kolommen steeds de specificaties uit deze verordening.

- U wordt verzocht in de derde kolom aan te geven hoe de specificaties zijn geïmplementeerd/ uitgewerkt voor wat betreft uw online verzamelsysteem.
- Gebruikt u de software van de Europese Commissie (OCS), dan zult u zien dat u diverse vragen kunt overslaan.
- Voor alle vragen die u moet invullen geldt dat, indien van toepassing en mogelijk, u het antwoord moet onderbouwen met documentatie.
- Gelieve de mee te sturen documentatie te rubriceren met het nummer van de technische specificatie waar deze betrekking op heeft.

Nr. in 1179	Specificatie in Verordening 1179/2011	U wordt verzocht in deze kolom aan te geven hoe invulling is gegeven aan de technische specificatie.
	TECHNISCHE SPECIFICATIES VOOR DE TENUITVOERLEGGING VAN ARTIKEL 6, LID 4, ONDER a), VAN VERORDENING (EU) Nr. 211/2011	*Niet invullen.*
1	Om geautomatiseerde indiening van steunbetuigingen via het systeem te voorkomen, moet de ondertekenaar, voor hij zijn steunbetuiging kan indienen, een passend verificatieproces volgen dat in overeenstemming is met de gangbare praktijk. Een van de mogelijke verificatieprocessen is het gebruik van een sterke uitvoering van het „Captcha"-systeem.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. Welk verificatieproces wordt toegepast? Functionele beschrijving en printscreen svp meesturen.
	TECHNISCHE SPECIFICATIES VOOR DE TENUITVOERLEGGING VAN ARTIKEL 6, LID 4, ONDER b), VAN VERORDENING (EU) Nr. 211/2011	*Niet invullen.*
	Normen voor informatiezekerheid	*Niet invullen.*
2.1	De organisatoren verstrekken documentatie waaruit blijkt dat zij voldoen aan de vereisten van de norm ISO/IEC 27001, maar zij hoeven zich voor deze norm niet formeel te laten certificeren. Om aan de norm te voldoen, dienen zij:	*Niet invullen.*

Nr. in 1179	Specificatie in Verordening 1179/2011	U wordt verzocht in deze kolom aan te geven hoe invulling is gegeven aan de technische specificatie.
	a) een volledige risicobeoordeling te hebben uitgevoerd, in het kader waarvan het toepassingsgebied van het systeem is vastgesteld, de gevolgen voor de activiteiten van allerlei inbreuken op de informatiezekerheid zijn aangegeven, de bedreigingen voor en kwetsbaarheden van het informatiesysteem zijn vermeld, een risicoanalyse is opgesteld die tegenmaatregelen noemt waarmee deze bedreigingen kunnen worden voorkomen en maatregelen die zullen worden genomen als een bedreiging zich voordoet, en tot slot een geprioriteerde lijst van verbeteringen is opgesteld;	Is er een uitgebreide risk assessment uitgevoerd met aandacht voor de genoemde onderwerpen? Documenten waaruit dit blijkt svp meezenden.
	b) maatregelen voor risicobehandeling te hebben opgezet en geïmplementeerd met betrekking tot de bescherming van persoonsgegevens en de bescherming van het familie- en gezinsleven en het privéleven, alsmede maatregelen die zullen worden genomen als een risico zich voordoet;	Zijn deze maatregelen opgezet en geïmplementeerd? Documenten waaruit dit blijkt svp meezenden.
	c) een schriftelijke opgave van de restrisico's te hebben gedaan;	Zijn restrisico's bepaald en schriftelijk vastgelegd? Documenten waaruit dit blijkt svp meezenden.
	d) te hebben voorzien in de organisatorische middelen om feedback te ontvangen over nieuwe bedreigingen en verbeteringen van de beveiliging.	Op welke wijze is hierin voorzien? Documenten waaruit dit blijkt svp meezenden.
2.2	Op basis van de risicoanalyse die overeenkomstig punt 2.1, onder a), is verricht, kiezen de organisatoren veiligheidsbeheersingsmaatregelen volgens een van de onderstaande normen:	*Niet invullen.*
	1. ISO/IEC 27002 of 2. de „Standard of Good Practice" van het Information Security Forum, om de volgende zaken aan te pakken:	Hier svp aangeven welk normenkader is gebruikt.
	a) risicobeoordelingen (aanbevolen wordt ISO/IEC 27005 of een andere specifieke geschikte beoordelingsmethodologie toe te passen);	Toelichting: een specifieke methodiek van risicobeoordeling is aanbevolen, maar niet verplicht. Hier svp aangeven op welke wijze en/of volgens welke methodiek de risicobeoordeling is uitgevoerd. Documenten waaruit dit blijkt svp meezenden.
	b) fysieke en omgevingsbeveiliging;	Hier svp aangeven welke maatregelen zijn genomen om aan dit punt te voldoen. Documenten waaruit dit blijkt svp meezenden.
	c) beveiliging in verband met de menselijke factor;	Hier svp aangeven welke maatregelen zijn genomen om aan dit punt te voldoen. Documenten waaruit dit blijkt svp meezenden.
	d) communicatie- en activiteitenbeheer;	Hier svp aangeven welke maatregelen zijn genomen om aan dit punt te voldoen. Documenten waaruit dit blijkt svp meezenden.
	e) standaardmaatregelen voor toegangscontrole, naast de maatregelen die in deze uitvoeringsverordening worden aangegeven;	Hier svp aangeven welke maatregelen zijn genomen om aan dit punt te voldoen. Documenten waaruit dit blijkt svp meezenden.
	f) aanschaf, ontwikkeling en onderhoud van informatiesystemen;	Hier svp aangeven welke maatregelen zijn genomen om aan dit punt te voldoen. Documenten waaruit dit blijkt svp meezenden.
	g) beheer van incidenten op het gebied van informatiebeveiliging;	Hier svp aangeven welke maatregelen zijn genomen om aan dit punt te voldoen. Documenten waaruit dit blijkt svp meezenden.
	h) maatregelen om inbreuken op informatiesystemen ongedaan te maken en de gevolgen ervan te verminderen, wanneer deze inbreuken kunnen leiden tot vernietiging, accidenteel verlies, vervalsing of ongeoorloofde bekendmaking van of ongeoorloofde toegang tot de verwerkte persoonsgegevens;	Hier svp aangeven welke maatregelen zijn genomen om aan dit punt te voldoen. Documenten waaruit dit blijkt svp meezenden.
	i) naleving van de voorschriften;	Hier svp aangeven welke maatregelen zijn genomen om aan dit punt te voldoen. Documenten waaruit dit blijkt svp meezenden.
	j) beveiliging van het computernetwerk (ISO/IEC 27033 of de reeds genoemde Standard of Good Practice wordt aanbevolen).	Hier svp aangeven welke maatregelen zijn genomen om aan dit punt te voldoen. Documenten waaruit dit blijkt svp meezenden.
	Functionele vereisten	**Indien u gebruikt maakt van OCS kunt u de normen 2.3 t/m 2.14 overslaan. Ga verder met norm 2.15**
2.3	Het systeem voor het online verzamelen van steunbetuigingen bestaat uit een instantie van een webtoepassing die is opgezet voor het verzamelen van steunbetuigingen aan één enkel burgerinitiatief.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. Wordt een webtoepassing gebruikt, bestaande uit één 'instance', opgezet voor het verzamelen van steunbetuigingen aan één enkel burgerinitiatief? Documenten waaruit dit blijkt svp meezenden.
2.4	Indien voor het beheer van het systeem verschillende rollen vereist zijn, wordt voorzien in verschillende toegangscontroleniveaus volgens het beginsel dat alleen strikt noodzakelijke rechten worden toegekend.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. Is hierin voorzien? Documenten waaruit dit blijkt svp meezenden.

Nr. in 1179	Specificatie in Verordening 1179/2011	U wordt verzocht in deze kolom aan te geven hoe invulling is gegeven aan de technische specificatie.
2.5	- Publiek toegankelijke voorzieningen zijn duidelijk afgescheiden van de voorzieningen die voor beheersdoeleinden bestemd zijn. - Er is geen toegangscontrole die verhindert dat de informatie in het publieke gedeelte van het systeem wordt gelezen; dit geldt onder meer voor informatie over het initiatief en voor het elektronische steunbetuigingsformulier. - Steunbetuigingen voor een initiatief kunnen uitsluitend via dit publieke gedeelte worden ingediend.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. Hier svp aangeven welke maatregelen zijn genomen om aan deze punten te voldoen Documenten waaruit dit blijkt svp meezenden.
2.6	Het systeem signaleert en voorkomt dat meer dan éénmaal een steunbetuiging wordt ingediend.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. Signaleert en voorkomt het systeem dat meer dan éénmaal een steunbetuiging wordt ingediend? Documenten waaruit dit blijkt svp meezenden.
	Beveiliging op toepassingsniveau	*Niet invullen.*
2.7	Het systeem wordt adequaat beschermd tegen bekende kwetsbaarheden en exploits. Daartoe moet het aan onder andere de volgende vereisten voldoen:	*Niet invullen.*
2.7.1	Het systeem wordt beschermd tegen injectie van zoekopdrachten via onder andere SQL (Structured Query Language), LDAP (Lightweight Directory Access Protocol), XPath (XML Path Language), opdrachten van het besturingssysteem of argumenten bij programma's. Daartoe is in ieder geval het volgende vereist:	*Niet invullen.* Hierna alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. U dient door middel van (de resultaten van) een uitgevoerde website penetratietest aan te tonen dat aan de punten a, b en c wordt voldaan.
	a) alle gebruikersinput wordt gevalideerd;	
	b) de validering wordt ten minste aan serverzijde uitgevoerd;	
	c) bij gebruik van interpreters worden niet-vertrouwde gegevens altijd gescheiden van (zoek)opdrachten. Voor SQL-opdrachten betekent dit dat bij alle prepared statements en stored procedures gebruik moet worden gemaakt van bindingsvariabelen en dat dynamische zoekopdrachten moeten worden vermeden.	
2.7.2	Het systeem wordt beschermd tegen cross-site scripting (XSS). Daartoe is in ieder geval het volgende vereist:	*Niet invullen.* Hierna alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. U dient door middel van een uitgevoerde website penetratietest aan te tonen dat aan de punten a, b en c hierna wordt voldaan.
	a) van alle gebruikersinput die naar de browser wordt teruggestuurd, wordt de veiligheid geverifieerd (door middel van validering van de input);	
	b) alle gebruikersinput wordt waar nodig voorzien van escape sequences, voordat deze in de outputpagina wordt opgenomen;	
	c) de output wordt zodanig gecodeerd dat de input door de browser altijd als tekst wordt behandeld. Er wordt geen actieve content gebruikt.	
2.7.3	Het systeem is voorzien van sterke authenticatie en sessiebeheer, waarvoor in ieder geval het volgende vereist is:	*Niet invullen* Hierna alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. U dient door middel van een uitgevoerde website penetratietest aan te tonen dat aan de punten a t/m h hierna wordt voldaan.
	a) inloggegevens worden bij opslag altijd beschermd door hashing of encryptie. Het risico dat authenticatie plaatsvindt door middel van „pass-the-hash" moet worden verminderd;	
	b) inloggegevens kunnen niet worden geraden of overschreven als gevolg van zwak accountbeheer (bv. account aanmaken, wachtwoord wijzigen, wachtwoord herstellen, zwakke sessie-identificatoren (sessie-id's));	
	c) sessie-id's en sessiegegevens worden niet weergegeven in de URL (Uniform Resource Locator);	
	d) sessie-id's zijn niet vatbaar voor aanvallen door middel van session fixation;	
	e) sessie-id's verstrijken, waardoor gebruikers worden uitgelogd;	
	f) sessie-id's worden na een succesvolle login niet opnieuw gebruikt;	
	g) wachtwoorden, sessie-id's en andere gegevens worden uitsluitend via Transport Layer Security (TLS) verzonden;	

Nr. in 1179	Specificatie in Verordening 1179/2011	U wordt verzocht in deze kolom aan te geven hoe invulling is gegeven aan de technische specificatie.
	h) Het beheersgedeelte van het systeem wordt afgeschermd. Als het wordt beschermd met enkelvoudige authenticatie, moet het wachtwoord uit ten minste tien tekens bestaan, waaronder ten minste één letter, één cijfer en één speciaal teken. Ook dubbele authenticatie kan worden gebruikt. Bij enkelvoudige authenticatie moet voor internettoegang tot het administratieve gedeelte van het systeem een verificatie in twee stappen worden toegepast: de enkelvoudige authenticatie wordt uitgebreid met een andere authenticatiemethode, zoals een via sms verzonden eenmalige wachtzin of wachtcode, of een asymmetrisch geëncrypteerde challenge in de vorm van een toevalsgetal, die wordt gedecrypteerd met de geheime sleutel van de organisatoren/administratoren, die bij het systeem niet bekend is.	
2.7.4	Het systeem bevat geen onveilige directe objectreferenties. Daartoe is in ieder geval het volgende vereist:	*Niet invullen* Hierna alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. U dient door middel van een uitgevoerde website penetratietest aan te tonen dat aan de punten a en b hierna wordt voldaan.
	a) voor directe referenties naar voorzieningen met restricties verifieert de toepassing of de gebruiker toegang mag worden verleend tot de gevraagde voorziening;	
	b) als het om een indirecte referentie gaat, wordt de mapping naar de directe referentie beperkt tot de waarden die voor de betrokken gebruiker zijn toegestaan.	
2.7.5	Het systeem wordt beschermd tegen cross-site request forgery.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. U dient door middel van een uitgevoerde website penetratietest aan te tonen dat hieraan voldaan wordt.
2.7.6	Het systeem is voorzien van een deugdelijke beveiligingsconfiguratie, waarvoor in ieder geval het volgende is vereist:	*Niet invullen.* De volgende vragen alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt.
	a) alle softwareonderdelen zijn up-to-date, inclusief het besturingssysteem, de web-/toepassingsserver, het databasemanagementsysteem (DBMS), de toepassingen en alle codelibrary's;	Op welke wijze wordt gewaarborgd dat softwarecomponenten up to date worden gehouden? Op welke wijze wordt gewaarborgd dat de web/application server en het operating system (OS) up to date zijn? Documenten waaruit blijkt dat alle software componenten up to date zijn svp meezenden.
	b) niet-benodigde services van het besturingssysteem en de web-/toepassingsserver zijn gedeactiveerd, verwijderd of niet geïnstalleerd;	U dient door middel van een uitgevoerde website penetratietest aan te tonen dat aan de punten b t/m e wordt voldaan.
	c) standaardwachtwoorden voor accounts zijn gewijzigd of de standaardaccounts gedeactiveerd;	
	d) de foutafhandeling is zodanig opgezet dat stack traces en andere te informatieve foutmeldingen niet worden doorgelaten;	
	e) de beveiligingsinstellingen van ontwikkelingsframeworks en -library's zijn conform de beste praktijken, zoals de richtsnoeren van OWASP.	
2.7.7	Gegevens in het systeem worden als volgt geëncrypteerd:	*Niet invullen* Hierna alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. U dient van de punten a t/m d hierna aan te geven welke maatregelen u getroffen heeft om te waarborgen dat aan de genoemde punten voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
	a) persoonsgegevens in elektronische vorm worden geëncrypteerd voor zij worden opgeslagen of verzonden naar de bevoegde autoriteiten van de lidstaten overeenkomstig artikel 8, lid 1, van Verordening (EU) nr. 211/2011. Beheer en back-up van de sleutels zijn daarvan gescheiden;	
	b) er wordt gebruikgemaakt van sterke standaardalgoritmen en sterke sleutels, die aan de internationale normen voldoen. Er is gezorgd voor sleutelbeheer;	
	c) wachtwoorden worden gehasht met een sterk standaardalgoritme en er wordt een passende saltwaarde gebruikt;	
	d) alle sleutels en wachtwoorden worden tegen ongeoorloofde toegang beschermd.	
2.7.8	Het systeem beperkt URL-toegang op basis van de toegangs- en gebruiksrechten van de gebruiker. Daartoe is in ieder geval het volgende vereist:	*Niet invullen* Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. U dient van de punten a en b hierna aan te geven welke maatregelen u getroffen heeft om te waarborgen dat aan de genoemde punten voldaan wordt. Documenten waaruit dit blijkt svp meezenden.

Nr. in 1179	Specificatie in Verordening 1179/2011	U wordt verzocht in deze kolom aan te geven hoe invulling is gegeven aan de technische specificatie.
	a) als de authenticatie- en autorisatiecontroles voor de toegang tot een pagina via externe beveiligingsmechanismen worden uitgevoerd, moeten deze voor elke pagina naar behoren zijn geconfigureerd;	
	b) als bescherming op codeniveau wordt gebruikt, moet die voor elke opgevraagde pagina gelden.	
2.7.9	Het systeem maakt gebruik van afdoende bescherming van de transportlaag. Daartoe zijn alle volgende maatregelen vereist, of maatregelen die ten minste even effectief zijn:	*Niet invullen* Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. U dient door middel van een uitgevoerde website penetratietest hieronder aan te tonen dat aan de punten a t/m c wordt voldaan.
	a) voor de toegang tot elke gevoelige voorziening vereist het systeem de meest recente versie van HTTPS (Hypertext Transfer Protocol Secure); de certificaten moeten geldig zijn, zij mogen niet zijn verstreken of ingetrokken en zij moeten overeenstemmen met alle domeinen die voor de site worden gebruikt;	
	b) het systeem stelt voor alle gevoelige cookies de flag „secure" in;	
	c) op de server is de TLS-provider zodanig geconfigureerd dat deze slechts de beste encryptiealgoritmen ondersteunt. De gebruikers wordt meegedeeld dat zij TLS-ondersteuning in hun browser moeten activeren.	
2.7.10	Het systeem wordt beschermd tegen ongeldig gemaakte redirects en forwards.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. U dient door middel van een uitgevoerde website penetratietest aan te tonen dat hieraan voldaan wordt.
	Databasebeveiliging en gegevensintegriteit	*Niet invullen.*
2.8	Als voor verschillende burgerinitiatieven systemen voor het online verzamelen van steunbetuigingen worden gebruikt die gebruikmaken van dezelfde hardware en besturingssysteemvoorzieningen, mogen nooit gegevens (met inbegrip van toegangs- of encryptiegegevens) worden gedeeld. Bovendien moeten de risicobeoordeling en de gebruikte tegenmaatregelen aan deze situatie zijn aangepast.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. Documenten waaruit dit blijkt svp meezenden.
2.9	Het risico dat authenticatie voor de database plaatsvindt door middel van „pass-the-hash" moet worden verminderd.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. U dient door middel van een uitgevoerde website penetratietest aan te tonen dat hieraan voldaan wordt.
2.10	De gegevens die de ondertekenaars verstrekken, mogen uitsluitend toegankelijk zijn voor de databaseadministrator of -beheerder.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. U dient door middel van een uitgevoerde website penetratietest aan te tonen dat hieraan voldaan wordt. U dient aan te geven welke maatregelen u getroffen heeft om te waarborgen dat hieraan voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
2.11	Beheersgegevens, persoonsgegevens die door ondertekenaars zijn opgegeven en back-ups daarvan worden beveiligd met sterke encryptiealgoritmen als bedoeld in punt 2.7.7, onder b). De lidstaat waar de steunbetuiging zal worden geteld, de datum waarop de steunbetuiging is ingediend en de taal waarin de ondertekenaar het formulier heeft ingevuld, mogen echter zonder encryptie in het systeem worden vermeld.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan de genoemde punten voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
2.12	De ondertekenaars mogen slechts toegang krijgen tot de gegevens die zij hebben opgegeven tijdens de sessie waarin zijn het steunbetuigingsformulier hebben ingevuld. Zodra de steunbetuiging is ingediend, wordt deze sessie afgesloten en zijn de ingediende gegevens niet langer toegankelijk.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan de genoemde punten voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
2.13	Persoonsgegevens van de ondertekenaar komen slechts in geëncrypteerde vorm in het systeem en in de back-up voor. Voor de raadpleging van gegevens of de certificering door de nationale autoriteiten overeenkomstig artikel 8 van Verordening (EU) nr. 211/2011 mogen de organisatoren de geëncrypteerde gegevens volgens punt 2.7.7, onder a), exporteren.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan de genoemde punten voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
2.14	De in het steunbetuigingsformulier ingevulde gegevens zijn slechts in hun totaliteit persistent in het systeem. Dat wil zeggen: wanneer de gebruiker alle vereiste gegevens in het steunbetuigingsformulier heeft ingevoerd en zijn besluit om het burgerinitiatief te steunen heeft gevalideerd, legt het systeem ofwel alle gegevens van het formulier volledig vast, ofwel geen van die gegevens, indien er een fout optreedt. Het systeem deelt de gebruiker mee of het verzoek al dan niet met succes is ingevoerd.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan de genoemde punten voldaan wordt. Documenten waaruit dit blijkt svp meezenden.

Nr. in 1179	Specificatie in Verordening 1179/2011	U wordt verzocht in deze kolom aan te geven hoe invulling is gegeven aan de technische specificatie.
2.15	Het databasemanagementsysteem is up-to-date en wordt voortdurend bijgewerkt wanneer nieuwe exploits worden ontdekt.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan de genoemde punten voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
2.16	Alle activiteitenlogs van het systeem zijn aanwezig.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan de genoemde punten voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
	Het systeem zorgt ervoor dat excepties en andere voor de beveiliging relevante gebeurtenissen, zoals hieronder genoemd, worden vermeld in auditlogs die kunnen worden getoond en worden behouden totdat de gegevens worden vernietigd overeenkomstig artikel 12, lid 3) of lid 5), van Verordening (EU) nr. 211/2011.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan de genoemde punten voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
	Deze logs worden op passende wijze beschermd, bijvoorbeeld door opslag op geëncrypteerde media.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan de genoemde punten voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
	De organisatoren/administratoren gaan regelmatig na of de logs op verdachte activiteiten wijzen.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan de genoemde punten voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
	In de logs worden ten minste de volgende gegevens opgenomen:	*Niet invullen.* Hierna svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan de genoemde punten a t/m c voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
	a) datum en tijdstip waarop de organisatoren/ administratoren inloggen en uitloggen;	
	b) verrichte back-ups;	
	c) alle door de administrator van de database aangebrachte wijzigingen en bijwerkingen.	
	Beveiliging van infrastructuur: fysieke locatie, netwerkinfrastructuur en serveromgeving	*Niet invullen.* Toelichting: normen en maatregelen binnen Infrastructure security kunnen afgedekt worden door een hosting contract (SLA). Een contract is niet verplicht.
2.17	*Fysieke beveiliging* Ongeacht het type hosting dient de machine waarop de toepassing wordt gehost, naar behoren te zijn beschermd, en wel op de volgende wijze:	*Niet invullen.* Hierna svp aangeven welke maatregelen voor de punten a t/m c getroffen zijn om het voldoen aan deze specificaties te borgen. Documenten waaruit dit blijkt svp meezenden.
	a) toegangscontrole en auditlog betreffende de toegang tot de hostingruimte;	
	b) fysieke bescherming van de back-upgegevens tegen diefstal en zoekraken;	
	c) opstelling van de server waarop de toepassing draait in een beveiligd rek.	
2.18	*Netwerkbeveiliging*	*Niet invullen.*
2.18.1	Het systeem wordt gehost op een met het internet verbonden server die geïnstalleerd is in een demilitarized zone (DMZ) en beveiligd wordt met een firewall.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan de genoemde punten voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
2.18.2	Wanneer relevante updates en patches voor het firewallproduct worden uitgebracht, worden deze zo spoedig mogelijk geïnstalleerd.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan het genoemde punt voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
2.18.3	Al het inkomende en uitgaande verkeer van de server (dat bestemd is voor het systeem) wordt aan de hand van de firewallregels gescreend en gelogd. De firewallregels houden alle verkeer tegen dat niet nodig is voor het veilige gebruik en beheer van het systeem.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan de genoemde punten voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
2.18.4	Het systeem voor het online verzamelen van steunbetuigingen wordt gehost op een afdoende beschermd productiesegment van het netwerk, dat afgescheiden is van segmenten waarop niet-productiesystemen worden gehost, zoals ontwikkelings- of testomgevingen.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan de genoemde punten voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
2.18.5	Het lokale netwerk (LAN) wordt beveiligd met maatregelen zoals:	*Niet invullen.* Hierna svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan de genoemde punten a t/m d voldaan wordt.
	a) toegangslijst voor de tweede laag (L2)/ poortbeveiliging;	
	b) deactivering van ongebruikte poorten;	
	c) de DMZ bevindt zich op een afzonderlijk virtueel netwerk (VLAN) of LAN;	
	d) er vindt geen L2-trunking plaats op niet-benodigde poorten.	
2.19	*Beveiliging van het besturingssysteem en de web-/ toepassingsserver*	*Niet invullen.*
2.19.1	De beveiliging is correct geconfigureerd met inachtneming van punt 2.7.6.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan de genoemde punten voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
2.19.2	De toepassingen worden uitgevoerd met slechts die rechten die voor hun functioneren noodzakelijk zijn.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan het genoemde punt voldaan wordt. Documenten waaruit dit blijkt svp meezenden.

Nr. in 1179	Specificatie in Verordening 1179/2011	U wordt verzocht in deze kolom aan te geven hoe invulling is gegeven aan de technische specificatie.
2.19.3	Bij toegang van een administrator tot de beheersinterface van het systeem geldt een korte sessietime-out (maximaal 15 minuten).	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan het genoemde punt voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
2.19.4	Wanneer relevante updates en patches voor het besturingssysteem, de toepassingsruntimes, de op de servers draaiende toepassingen of malwarepreventiesoftware worden uitgebracht, worden deze zo spoedig mogelijk geïnstalleerd.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan het genoemde punt voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
2.19.5	Het risico dat authenticatie voor de database plaatsvindt door middel van „pass-the-hash" moet worden verminderd.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan het genoemde punt voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
2.20	*Beveiliging van de door de organisatoren gebruikte clients* Om ervoor te zorgen dat het hele systeem van begin tot einde is beveiligd, nemen de organisatoren maatregelen ter beveiliging van de clienttoepassing of de machine die zij gebruiken voor het beheer van en de toegang tot het systeem voor het online verzamelen van steunbetuigingen, zoals de hierna volgende.	*Niet invullen.*
2.20.1	Niet-beheerstaken (zoals inzake kantoorautomatisering) worden uitgevoerd met slechts die rechten die voor hun functioneren noodzakelijk zijn.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan het genoemde punt voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
2.20.2	Wanneer relevante updates en patches voor het besturingssysteem, geïnstalleerde toepassingen of malwarepreventie worden uitgebracht, worden deze zo spoedig mogelijk geïnstalleerd.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan het genoemde punt voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
	TECHNISCHE SPECIFICATIES VOOR DE TENUITVOERLEGGING VAN ARTIKEL 6, LID 4, ONDER c), VAN VERORDENING (EU) Nr. 211/2011	*Niet invullen*
3.1	Het systeem voorziet in de mogelijkheid om voor elke afzonderlijke lidstaat een rapport op te stellen waarin voor het burgerinitiatief de persoonsgegevens van de ondertekenaars zijn opgenomen, zodat de bevoegde autoriteiten van de betrokken lidstaat deze kunnen verifiëren.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan het genoemde punt voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
3.2	De door de ondertekenaars ingediende steunbetuigingen kunnen worden geëxporteerd in het formaat van bijlage III bij Verordening (EU) nr. 211/2011. Het systeem mag daarnaast in de mogelijkheid voorzien om de steunbetuigingen te exporteren in een interoperabel formaat zoals xml (Extensible Markup Language).	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan het genoemde punt voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
3.3	De geëxporteerde steunbetuigingen worden met als rubricering *beperkte verspreiding* aan de betrokken lidstaat ter beschikking gesteld en aangemerkt als *persoonsgegevens*.	Alleen beantwoorden als u i.p.v. OCS een andere applicatie gebruikt. Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan het genoemde punt voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
3.4	De elektronische verzending van de geëxporteerde gegevens naar de lidstaten wordt tegen afluisteren beschermd door middel van geschikte end-to-endencryptie.	Hier svp aangeven welke maatregelen getroffen zijn om te waarborgen dat aan het genoemde punt voldaan wordt. Documenten waaruit dit blijkt svp meezenden.
	OVERIG	*Niet invullen.*
Overweging (6)	Het certificeringsproces wordt vergemakkelijkt indien de organisatoren gebruikmaken van de software die de Commissie verstrekt overeenkomstig artikel 6, lid 2, van Verordening (EU) nr. 211/2011.	Toelichting: het certificeringsproces wordt alleen vergemakkelijkt indien de organisatoren *ongewijzigd* gebruikmaken van de software die de Commissie verstrekt. Daarom hier svp aangeven of de hash van OCS niet is veranderd. Documenten waaruit dit blijkt svp meezenden.
	Het onlinesysteem wordt overeenkomstig Verordening (EU) nr. 211/2011 gecertificeerd in de lidstaat waar de middels het onlinesysteem verzamelde gegevens worden opgeslagen.	Hier svp aangeven dat de data worden opgeslagen in Nederland. Documenten waaruit dit blijkt svp meezenden.

TOELICHTING

Deze regeling ziet op de uitwerking van artikel 3 van de Uitvoeringswet verordening Europees burgerinitiatief (Stb. 2013, 318). In dit artikel is bepaald dat bij ministeriële regeling zal worden vastgelegd welke gegevens en bescheiden in ieder geval moeten worden overgelegd bij een aanvraag voor een certificaat van een online verzamelsysteem waarmee steunbetuigingen voor een Europees burgerinitiatief kunnen worden verzameld. Een aanvraag voor een dergelijk certificaat wordt ingediend bij de minister van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK). Indien de aanvraag volledig is wordt deze in behandeling genomen (artikel 4:5 van de Algemene wet bestuursrecht) en vervolgens wordt binnen een maand op de aanvraag besloten (artikel 6, derde lid, van Verordening (EU) nr. 211/2011 van het Europees Parlement en de Raad van 16 februari 2011 over het burgerinitiatief (PbEU 2011, L 65 (hierna: de Verordening)).

In deze regeling is voorgeschreven dat bij het indienen van de aanvraag een volledig ingevuld aanvraagformulier (bijlage 1) en vragenlijst (bijlage 2) moeten worden verstrekt, inclusief de op grond van deze bijlagen verplichte documenten. De Uitvoeringsverordening (EU) nr. 1179/2011 van de Commissie van 17 november 2011 tot vaststelling van technische specificaties voor systemen voor het online verzamelen van steunbetuigingen overeenkomstig Verordening (EU) nr. 211/2011 van het Europees Parlement en de Raad over het burgerinitiatief (PbEU 2011, L 301) (hierna: de Uitvoeringsverordening) stelt zeer specifieke technische en veiligheidseisen aan het systeem en die vormen het uitgangspunt bij deze regeling. De technische en veiligheidseisen aan het online verzamelsysteem zijn om meerdere redenen noodzakelijk: in dit verzamelsysteem worden privacygevoelige persoonsgegevens opgeslagen, geautomatiseerde indiening moet worden voorkomen en steunbetuigingen moeten niet ongewenst verwijderd kunnen worden.
Het is van groot belang dat organisatoren bij de aanvraag de relevante informatie en documentatie leveren waaruit kan blijken dat het systeem aan de vereisten voldoet. Er wordt hierbij één op één aangesloten bij de vereisten in de Verordening en de Uitvoeringsverordening. Mede op basis van deze informatie en documentatie kan worden vastgesteld hoeveel aanvullend (fysiek) onderzoek er nodig is om te beoordelen in hoeverre het systeem aan de vereisten voldoet. Het ministerie van BZK onderhoudt alvorens en tijdens het proces van certificering nauw contact met het organisatiecomité van een Europees burgerinitiatief dat een verzoek tot certificering aan de minister heeft gericht of wenst te richten. Indien een organisatiecomité daar prijs op stelt kan er op ambtelijk niveau een onderhoud gepland worden om (mondeling) een toelichting te verschaffen op de noodzakelijke technische en veiligheidsmaatregelen voor het online verzamelsysteem en de vereiste informatie en documentatie.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk.