

DESCRIPTION OF CERTIFICATION OF AN INFORMATION SYSTEM FOR COLLECTION OF STATEMENTS OF SUPPORT

I. GENERAL PROVISIONS

1. This description of certification of information system for collection of statements of support (hereinafter – the description) regulates the procedure of certification of statements of support collection's information system.

2. The main concepts are used in a way, within the meaning of the European Parliament and the Council in the Regulation (EU) No 211/2011 of 16 February 2011 on citizens' initiatives (OL 2011 L 65, p. 1), in the Commission Implementing Regulation (EU) No 1179/2011 of November the 17th (OL 2011 L301, p. 3) and in the change and complements of the 2, 3 articles Republic of Lithuania Law on the Central Electoral Commission (hereinafter – The Law).

II. CERTIFICATION OF THE SYSTEM

3. In order to certify an information system for collection of statements of support, the organisers of the European Union citizens' initiative (hereinafter – the Organisers), shall submit to the Central Electoral Commission:

3.1. a request for Certification of an online system for collection of statements of support;

3.2. a declaration for Certification of an online system for collection of statements of support, which coincides with the Regulation (1 Annex), which is submitted with these documents:

3.2.1. a risk analysis report;

3.2.2. compliance with the requirements set out in the Commission's Implementing Regulation (EU) No 1179/2011 and conformity assessment of compliance with necessary requirements of the standard *ISO27001* (2 Annex)

3.2.3. a report on vulnerabilities assessment;

3.2.4. a report on intrusion test;

3.2.5. a statement about the Organiser's registration of personal data in in the registry of the country.

4. The documents laid down in points 3.2.1., 3.2.2., 3.2.3. and 3.2.4. shall be verified by the certified information technologies auditor.

5. The organisers shall submit the certificate, which confirms qualification of the information technologies auditor (CISA, CISM or any internationally recognized certificate).

III. FINAL PROVISIONS

6. The Central Electoral Commission in a course of one month after the date of the received request, having verified that information system for collection of statements of support meets the requirements, issues a certificate, which confirms compliance with the requirements of a Regulation.

7. The legal acts of the Republic of Lithuania give responsibilities for infringements of the legal acts, related to the European Union citizens' initiative and processing of personal data, are provided in

**DECLARATION FOR AN ONLINE COLLECTION SYSTEM OF STATEMENTS OF
SUPPORT COMPLIANCE WITH A REGULATION**

(date)

Organisers of the European Union citizens' initiative declare, that statements of support collection's online system ... (*website address*) for the collection of statements of support (name of the requested citizens' initiative) complies with:

- a) provisions of the related Regulation (EU) No 211/2011;
- b) requirements provided in the Commission's implementation Regulation (EU) No 1179/2011.

Data is stored in the data centre of the statements of support collection's online system ... (*data centre's website*), which is managed by (*name of the data centre's governor*).

A list of submitted documents:

- 1) a Report on risk analysis;
- 2) a Conformity assessment;
- 3) a vulnerabilities assessment report;
- 4) an intrusion test report;
- 5) a certificate, which confirms qualification of information technologies auditors.

The organiser of the European Union citizens' initiative

(full name)

(signature)

Assessment for compliance with the requirements of the information system, set out on 17
November 2011 in the Commission's Implementation Regulation (EU) No 1179/2011 and
compliance with the necessary requirements of the standard *ISO27001*

Area of the requirements	A list of necessary requirements (Points of the Regulation (EU) No 1179/2011)	
	When the software, which was prepared by the Commission according to the Regulation (EU) No 211/2011 Article 6 2nd part, is being used	When other software is being used
Standards of information security	2.1 2.2	2.1 2.2
Functional requirements	–	2.3 2.4 2.5 2.6
Security level of the programme	2.7.3.g 2.7.4. 2.7.4.a 2.7.4.b 2.7.9.a 2.7.9.b 2.7.9.c 2.19.3 2.16 2.7.6 2.15 2.17 2.18.1 2.18.2 2.18.3 2.18.4 2.18.5 2.19.4 2.20 2.20.1 2.20.2 2.19.1 2.19.5	2.7.1 2.7.1.a 2.7.1.b 2.7.1.c 2.7.2.a 2.7.2.b 2.7.2.c 2.7.3 2.7.3.a 2.7.3.b 2.7.3.c 2.7.3.d 2.7.3.e 2.7.3.f 2.7.7.a 2.7.7.b 2.7.7.c 2.7.7.d 2.11 2.13 2.7.8.a 2.7.8.b 2.7.3.h 2.12 2.8 2.10 2.19.2 2.14 2.7.3.g 2.7.4. 2.7.4.a 2.7.4.b 2.7.9.a 2.7.9.b

		2.7.9.c 2.19.3 2.16 2.7.6 2.15 2.17 2.18.1 2.18.2 2.18.3 2.18.4 2.18.5 2.19.4 2.20 2.20.1 2.20.2 2.7.5 2.7.10 2.9 2.19.1 2.19.5
Technical specificities of implementation the Regulation (EU) No 211/2011 Article 6 4th part point c	3.4	3.1 3.2 3.3 3.4
Compliance with the standard <i>ISO27001</i> of the implemented security measures		
Security measures	A list of necessary requirements (Points of the standard <i>ISO/IEC 27001:2005</i>)	
	7.1	7.1
	9.1	9.1
	9.2	9.2
	10.2	10.2
	10.3	10.3
	10.4	10.4
	10.5	10.5
	10.6	10.6
	10.7	10.7
	10.8	10.8
	10.10	10.10
	11.2	11.2
	11.4	11.4
	11.5	11.5
	11.6	11.6
	12.1	12.1
	12.3	12.3
	12.4	12.4
	12.6	12.6
	13.1	13.1
	13.2	13.2
	14.1	14.1
	15.1	15.1
	15.2	15.2