# Commission Implementing Regulation (EU) No 1179/2011 of 17 November 2011 laying down technical specifications for online collection systems pursuant to Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative

## COMMISSION IMPLEMENTING REGULATION (EU) No 1179/2011

## of 17 November 2011

## laying down technical specifications for online collection systems pursuant to Regulation (EU) No 211/2011 of the European Parliament and of the Council on the citizens' initiative

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative[(1)], and in particular Article 6(5) thereof,

After consulting the European Data Protection Supervisor,

Whereas:

(1) Regulation (EU) No 211/2011 provides that where statements of support are collected online, the system used for that purpose must satisfy certain security and technical requirements and must be certified by the competent authority of the relevant Member State.

(2) An online collection system within the meaning of Regulation (EU) No 211/2011 is an information system, consisting of software, hardware, hosting environment, business processes and staff in order to accomplish the online collection of statements of support.

(3) Regulation (EU) No 211/2011 sets out the requirements that online collection systems have to comply with in order to be certified and provides that the Commission should adopt technical specifications for implementing those requirements.

(4) The Open Web Application Security Project's (OWASP) Top 10 2010 project provides an overview of the most critical web application security risks as well as tools for addressing these risks; the technical specifications therefore draw upon the findings of this project.

(5) Implementation by the organisers of the technical specifications should guarantee certification of the online collection systems by the Member States' authorities, and contribute to ensure the implementation of the appropriate technical and organisational measures required to comply with the obligations imposed by Directive 95/46/EC of the European Parliament and of the Council[(2)] on the security of the processing activities, both at the time of the design of the processing system and at the time of the processing itself, in order to maintain security and thereby to prevent any unauthorised processing

**Changes to legislation:** *There are currently no known outstanding effects for the Commission Implementing Regulation (EU) No 1179/2011. (See end of Document for details)*

and protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

(6) The process of certification should be facilitated by the use by the organisers of the software provided by the Commission in accordance with Article 6(2) of Regulation (EU) No 211/2011.

(7) Organisers of citizens' initiatives, as data controllers, should, when collecting statements of support online, implement the technical specifications set out in this Regulation in order to ensure the protection of personal data processed. Where the processing is carried out by a processor, the organisers should ensure that the processor acts only on instructions from the organisers and that he implements the technical specifications set out in this Regulation.

(8) This Regulation respects fundamental rights and observes the principles enshrined in the Charter of Fundamental Rights of the European Union, in particular Article 8 thereof, which states that everyone has the right to the protection of personal data concerning him or her.

(9) The measures provided for in this Regulation are in accordance with the opinion of the Committee established under Article 20 of Regulation (EU) No 211/2011,

HAS ADOPTED THIS REGULATION:

*Article 1*

The technical specifications referred to in Article 6(5) of Regulation (EU) No 211/2011 are set out in the Annex.

*Article 2*

This Regulation shall enter into force on the 20th day following its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 17 November 2011.

*For the Commission*

*The President*

José Manuel BARROSO

***Changes to legislation:** There are currently no known outstanding effects for the Commission Implementing Regulation (EU) No 1179/2011. (See end of Document for details)*

# ANNEX

## 1. TECHNICAL SPECIFICATIONS AIMING AT IMPLEMENTING ARTICLE 6(4)(a) OF REGULATION (EU) No 211/2011

In order to prevent automated submission of a statement of support using the system, the signatory goes through an adequate verification process in line with current practice before submission of a statement of support. One possible verification process is the use of strong 'captcha'.

## 2. TECHNICAL SPECIFICATIONS AIMING AT IMPLEMENTING ARTICLE 6(4)(b) OF REGULATION (EU) No 211/2011

**Information assurance standards**

2.1. Organisers provide documentation showing that they fulfil the requirements of standard ISO/IEC 27001, short of adoption. For that purpose, they have:

(a) performed a full risk assessment, which identifies the scope of the system, highlights business impact in case of various breaches in information assurance, enumerates the threats and vulnerabilities of the information system, produces a risk analysis document that also list countermeasures to avoid such threats and remedies that will be taken if a threat occurs, and finally draws up a prioritised list of improvements;

(b) designed and implemented measures for treating risks with regard to the protection of personal data and the protection of family and private life and measures that will be taken in the case risk occurs;

(c) identified the residual risks in writing;

(d) provided the organisational means to receive feedback on new threats and security improvements.

2.2. Organisers choose security controls based on the risk analysis in 2.1(a) from the following standards:

(1) ISO/IEC 27002; or

(2) the Information Security Forum's 'Standard of Good Practice'

to address the following issues:

(a) risk assessments (ISO/IEC 27005 or another specific and suitable risk assessment methodology are recommended);

(b) physical and environmental security;

(c) human resources security;

(d) communications and operations management;

(e) standard access control measures, in addition to those set forth in this Regulation;

(f) information systems acquisition, development and maintenance;

(g) information security incident management;

**Changes to legislation:** *There are currently no known outstanding effects for the Commission Implementing Regulation (EU) No 1179/2011. (See end of Document for details)*

(h) measures to remedy and mitigate breaches in information systems which would result in the destruction or accidental loss, alteration, unauthorised disclosure or access of personal data processed;

(i) compliance;

(j) computer network security (ISO/IEC 27033 or the SoGP are recommended).

Application of these standards can be limited to the parts of the organisation that are relevant for the online collection system. For instance, human resources security can be limited to any staff that has physical or networking access to the online collection system, and physical/environmental security can be limited to the building(s) hosting the system.

**Functional requirements**

2.3. The online collection system consists of a web-based application instance set up for the purpose of collecting statements of support for a single citizens' initiative.

2.4. If administering the system requires different roles, then different levels of access control are established according to the principle of least privilege.

2.5. The publicly accessed features are clearly separated from the features destined for administration purposes. No access control hinders reading of the information available in the public area of the system, including information on the initiative and the electronic statement of support form. Signing up for an initiative is possible only via this public area.

2.6. The system detects and prevents submission of duplicate statements of support.

**Application level security**

2.7. The system is suitably protected against known vulnerabilities and exploits. For this purpose it satisfies, inter alia, the following requirements:

2.7.1. The system guards against injection flaws such as structured query language (SQL) queries, lightweight directory access protocol (LDAP) queries, XML path language (XPath) queries, operating system (OS) commands or program arguments. For this purpose, it requires at least that:

(a) all user input is validated;

(b) validation is performed at least by the server-side logic;

(c) all use of interpreters clearly separates untrusted data from the command or query. For SQL calls, this means using bind variables in all prepared statements and stored procedures, and avoiding dynamic queries.

2.7.2. The system guards against cross-site scripting (XSS). For this purpose, it requires at least that:

(a) all user supplied input sent back to the browser is verified to be safe (via input validation);

(b) all user input is properly escaped before it is included in the output page;

(c) proper output encoding ensures that such input is always treated as text in the browser. No active content is used.

2.7.3. The system has strong authentication and session management, which requires at least that:

***Changes to legislation:** There are currently no known outstanding effects for the Commission Implementing Regulation (EU) No 1179/2011. (See end of Document for details)*

(a) credentials are always protected when stored using hashing or encryption. The risk that someone authenticates using 'pass-the-hash' is mitigated;

(b) credentials cannot be guessed or overwritten through weak account management functions (e.g. account creation, change password, recover password, weak session identifiers (IDs));

(c) session IDs and session data are not exposed in the uniform resource locator (URL);

(d) session IDs are not vulnerable to session fixation attacks;

(e) session IDs timeout, which ensures that users log out;

(f) session IDs are not rotated after successful login;

(g) passwords, session IDs, and other credentials are sent only over transport layer security (TLS);

(h) the administration part of the system is protected. If it is protected by single-factor authentication, then the password is composed of a minimum of 10 characters, including at least one letter, one number and one special character. Alternatively two-factor authentication may be used. Where only single-factor authentication is used, it includes a two-step verification mechanism for accessing the administration part of the system via the Internet, in which the single factor is augmented by another means of authentication, such as a one-time pass-phrase/code via SMS or an asymmetrically encrypted random challenge string to be decrypted using the organisers'/administrators' private key unknown to the system.

2.7.4. The system does not have insecure direct object references. For this purpose, it requires at least that:

(a) for direct references to restricted resources, the application verifies that the user is authorised to access the exact resource requested;

(b) if the reference is an indirect reference, the mapping to the direct reference is limited to values authorised for the current user.

2.7.5. The system guards against cross-site request forgery flaw.

2.7.6. Proper security configuration is in place, which requires, at least, that:

(a) all software components are up to date, including the OS, web/application server, database management system (DBMS), applications, and all code libraries;

(b) OS and web/application server unnecessary services are disabled, removed, or not installed;

(c) default account passwords are changed or disabled;

(d) error handling is set up to prevent stack traces and other overly informative error messages from leaking;

(e) security settings in the development frameworks and libraries are configured in accordance with best practices, such as the guidelines of OWASP.