II

(Non-legislative acts)

REGULATIONS

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 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,

[1] OJ L 65, 11.3.2011, p. 1.

[2] OJ L 281, 23.11.1995, p. 31.

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

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;

(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:

(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.

2.7.7. The system provides for encryption of data as follows:

(a) personal data in electronic format is encrypted when stored or transferred to the competent authorities of the Member States in accordance with Article 8(1) of Regulation (EU) No 211/2011, the keys being managed and backed up separately;

(b) strong standard algorithms and strong keys are used in line with international standards. Key management is in place;

(c) passwords are hashed with a strong standard algorithm and an appropriate 'salt' is used;

(d) all keys and passwords are protected from unauthorised access.

2.7.8. The system restricts URL access based on the user access levels and permissions. For this purpose, it requires at least that:

(a) if external security mechanisms are used to provide authentication and authorisation checks for page access, they need to be properly configured for every page;

(b) if code level protection is used, code level protection needs to be in place for every required page.

2.7.9. The system uses sufficient transport layer protection. For this purpose, all of the following measures or measures of at least equal strength are in place:

(a) the system requires the most current version of the hypertext transfer protocol secure (HTTPS) to access any sensitive resource using certificates that are valid, not expired, not revoked, and match all domains used by the site;

(b) the system sets the 'secure' flag on all sensitive cookies;

(c) the server configures the TLS provider to only support encryption algorithms in line with best practices. The users are informed that they must enable TLS support in their browser.

2.7.10. The system guards against invalidated redirects and forwards.

Database security and data integrity

2.8. Where online collection systems used for different citizens' initiatives share hardware and operating system resources, they do not share any data, including access/encryption credentials. In addition, this is reflected in the risk assessment and in the implemented countermeasures.

2.9. The risk that someone authenticates on the database using 'pass-the-hash' is mitigated.

2.10. The data provided by the signatories is only accessible to the database administrator/organiser.

2.11. Administrative credentials, personal data collected from signatories and its backup are secured via strong encryption algorithms in line with point 2.7.7(b). However, the Member State where the statement of support will be counted, the date of submission of the statement of support and the language in which the signatory filled in the statement of support form may be stored unencrypted in the system.

2.12. Signatories only have access to the data submitted during the session in which they complete the statement of support form. Once the statement of support form is submitted the above session is closed and the submitted data is not accessible anymore.

2.13. Signatories' personal data are only available in the system, including the backup, in encrypted format. For the purpose of data consultation or certification by the national authorities in accordance with Article 8 of Regulation (EU) No 211/2011, organisers may export the encrypted data in accordance with point 2.7.7(a).

2.14. The persistence of the data entered in the statement of support form is atomic. That is, once the user has entered all required details in the statement of support form, and validates his/her decision to support the initiative, the system either successfully commits all of the form data to the database, or, in case of error, fails by saving no data at all. The system informs the user of the success or failure of his/her request.

2.15. The DBMS used is up to date and continuously patched for newly discovered exploits.

2.16. All system activity logs are in place. The system makes sure that audit logs recording exceptions and other security-relevant events listed below may be produced and kept until the data is destroyed in accordance with Article 12(3) or (5) of Regulation (EU) No 211/2011. Logs are adequately protected, for instance by storage on encrypted media. Organisers/administrators regularly check the logs for suspicious activity. Log contents include at least:

(a) dates and times for log-on and log-off by organisers/administrators;

(b) performed backups;

(c) all database administrator changes and updates.

Infrastructure security — physical location, network infrastructure and server environment

2.17. *Physical security*

Whatever the type of hosting used, the machine hosting the application is properly protected, which provides:

(a) hosting area access control and audit log;

(b) physical protection of backup data against theft or incidental misplacement;

(c) that the server hosting the application is installed in a secured rack.

2.18. *Network security*

2.18.1. The system is hosted on an Internet facing server installed on a demilitarised zone (DMZ) and protected by a firewall.

2.18.2. When relevant updates and patches of the firewall product become public, then such updates or patches are installed expediently.

2.18.3. All inbound and outbound traffic to the server (destined to the online collection system) is inspected by the firewall rules and logged. The firewall rules deny all traffic that is not needed for the secure use and administration of the system.

2.18.4. The online collection system must be hosted on an adequately protected production network segment that is separated from segments used to host non-production systems such as development or testing environments.

2.18.5. Local area network (LAN) security measures are in place such as:

(a) layer 2 (L2) access list/port switch security;

(b) unused switch ports are disabled;

(c) the DMZ is on a dedicated virtual local area network (VLAN)/LAN;

(d) no L2 trunking enabled on unnecessary ports.

2.19. *OS and web/application server security*

2.19.1. A proper security configuration is in place including the elements listed in point 2.7.6.

2.19.2. Applications run with the lowest set of privileges that they require to run.

2.19.3. Administrator access to the management interface of the online collection system has a short session time-out (maximum 15 minutes).

2.19.4. When relevant updates and patches of the OS, the application runtimes, applications running on the servers, or anti-malware become public, then such updates or patches are installed expediently.

2.19.5. The risk that someone authenticates on the system using 'pass-the-hash' is mitigated.

2.20. *Organiser client security*

For the sake of end-to-end security, the organisers take necessary measures to secure their client application/device that they use to manage and access the online collection system, such as:

2.20.1. Users run non-maintenance tasks (such as office automation) with the lowest set of privileges that they require to run.

2.20.2. When relevant updates and patches of the OS, any installed applications, or anti-malware become public, then such updates or patches are installed expediently.

3. TECHNICAL SPECIFICATIONS AIMING AT IMPLEMENTING ARTICLE 6(4)(c) OF REGULATION (EU) No 211/2011

3.1. The system provides the possibility to extract for each individual Member State a report listing the initiative and the personal data of the signatories subject to verification by the competent authority of that Member State.

3.2. Exporting of signatories' statements of support is possible in the format of Annex III to Regulation (EU) No 211/2011. The system may in addition provide for the possibility of exporting the statements of support in an interoperable format such as the extensible mark-up language (XML).

3.3. The exported statements of support are marked as being of *limited distribution* to the Member State concerned, and labelled as *personal data*.

3.4. The electronic transmission of exported data to the Member States is secured against eavesdropping using suitable end-to-end encryption.