II

*(Actes non législatifs)*

# RÈGLEMENTS

## RÈGLEMENT D'EXÉCUTION (UE) Nº 1179/2011 DE LA COMMISSION

**du 17 novembre 2011**

**établissant des spécifications techniques pour les systèmes de collecte en ligne conformément au règlement (UE) nº 211/2011 du Parlement européen et du Conseil relatif à l'initiative citoyenne**

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) nº 211/2011 du Parlement européen et du Conseil du 16 février 2011 relatif à l'initiative citoyenne [1], et notamment son article 6, paragraphe 5,

après consultation du Contrôleur européen de la protection des données,

considérant ce qui suit:

(1) Le règlement (UE) nº 211/2011 prévoit que lorsque les déclarations de soutien sont recueillies en ligne, le système utilisé à cette fin doit satisfaire à certaines exigences en matière de sécurité et sur le plan technique et doit être certifié par l'autorité compétente de l'État membre concerné.

(2) Un système de collecte en ligne au sens du règlement (UE) nº 211/2011 est un système d'information composé d'un logiciel, de matériel, d'un environnement d'hébergement, de processus métier et de professionnels propres à assurer la collecte en ligne des déclarations de soutien.

(3) Le règlement (UE) nº 211/2011 établit les exigences auxquelles les systèmes de collecte en ligne doivent satisfaire pour pouvoir être certifiés et prévoit que la Commission adopte des spécifications techniques pour la mise en œuvre de ces exigences.

(4) Le Top 10 2010 de l'OWASP (*Open Web Application Security Project*) donne une vue d'ensemble des risques de sécurité applicatifs web les plus critiques ainsi que des outils permettant de faire face à ces risques. Les spécifications techniques s'appuient sur les résultats de ce projet.

(5) La mise en œuvre des spécifications techniques par les organisateurs devrait garantir la certification des systèmes de collecte en ligne par les autorités des États membres et contribuer à assurer l'application des mesures techniques et organisationnelles nécessaires au respect des obligations imposées par la directive 95/46/CE du Parlement européen et du Conseil [2] en ce qui concerne la sécurité des activités de traitement, tant au moment de la conception du système de traitement qu'au moment du traitement proprement dit, afin de préserver la sécurité et, ainsi, de prévenir tout traitement non autorisé et de protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la communication ou l'accès non autorisés.

(6) L'utilisation, par les organisateurs, du logiciel fourni par la Commission conformément à l'article 6, paragraphe 2, du règlement (UE) nº 211/2011 devrait faciliter le processus de certification.

(7) Les organisateurs d'initiatives citoyennes, tout comme les responsables du traitement, devraient, lorsqu'ils recueillent des déclarations de soutien en ligne, mettre en œuvre les spécifications techniques établies dans le présent règlement afin de garantir la protection des données à caractère personnel traitées. Lorsque le traitement est effectué par un sous-traitant, les organisateurs devraient veiller à ce que ce dernier n'agisse que sur leur seule instruction et à ce qu'il mette en œuvre les spécifications techniques prévues par le présent règlement.

(8) Le présent règlement respecte les droits fondamentaux et observe les principes consacrés par la charte des droits fondamentaux de l'Union européenne, notamment son article 8, qui dispose que toute personne a droit à la protection des données à caractère personnel la concernant.

(9) Les mesures prévues par le présent règlement sont conformes à l'avis du comité institué par l'article 20 du règlement (UE) nº 211/2011,

[1] JO L 65 du 11.3.2011, p. 1.

[2] JO L 281 du 23.11.1995, p. 31.

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

*Article premier*

Les spécifications techniques mentionnées à l'article 6, paragraphe 5, du règlement (UE) n° 211/2011 sont établies en annexe.

*Article 2*

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 17 novembre 2011.

*Par la Commission*
*Le président*
José Manuel BARROSO

*ANNEXE*

1. SPÉCIFICATIONS TECHNIQUES VISANT À METTRE EN ŒUVRE L'ARTICLE 6, PARAGRAPHE 4, POINT a), DU RÈGLEMENT (UE) Nº 211/2011

Afin d'empêcher toute utilisation du système aux fins de la présentation automatisée d'une déclaration de soutien, le signataire est soumis à un processus de vérification adéquat, conforme aux pratiques actuelles, avant la présentation d'une telle déclaration. Ce processus de vérification peut consister en l'utilisation d'un «captcha» complexe.

2. SPÉCIFICATIONS TECHNIQUES VISANT À METTRE EN ŒUVRE L'ARTICLE 6, PARAGRAPHE 4, POINT b), DU RÈGLEMENT (UE) Nº 211/2011

**Normes relatives à l'assurance de l'information**

2.1. Les organisateurs fournissent des documents prouvant qu'ils satisfont aux exigences de la norme ISO/CEI 27001, sans être tenus de l'adopter. À cette fin, ils ont:

a) réalisé une évaluation complète des risques, qui décrit l'étendue du système, met en lumière les incidences sur les activités en cas de diverses failles en matière d'assurance de l'information, énumère les vulnérabilités du système d'information et les menaces qui pèsent sur lui, débouche sur l'établissement d'un document d'analyse des risques qui recense les contre-mesures ayant pour but de parer à ces menaces et les solutions qui seront mises en œuvre si une menace se concrétise et, enfin, dresse une liste d'améliorations, classées par ordre de priorité;

b) élaboré et mis en œuvre des mesures pour faire face aux risques concernant la protection des données à caractère personnel et la protection de la vie familiale et de la vie privée, et défini les mesures à prendre lorsque le risque survient;

c) déterminé les risques résiduels par écrit;

d) mis en place des moyens organisationnels propres à permettre un retour d'information sur les nouvelles menaces et les nouvelles améliorations de la sécurité.

2.2. Les organisateurs choisissent des contrôles de sécurité fondés sur l'analyse de risque décrite au point 2.1 a) sur la base des normes suivantes:

1) la norme ISO/CEI 27002; ou

2) la norme de bonne pratique (*Standard of Good Practice* ou SoGP) élaborée par le *Information Security Forum*

pour veiller aux aspects suivants:

a) évaluations des risques (il est recommandé d'appliquer la norme ISO/CEI 27005 ou une autre méthode spécifique et appropriée d'évaluation des risques);

b) sécurité physique et environnementale;

c) sécurité des ressources humaines;

d) gestion des communications et opérations;

e) mesures standard de contrôle d'accès, en plus de celles décrites dans le présent règlement d'exécution;

f) acquisition, développement et maintenance des systèmes d'information;

g) gestion des incidents de sécurité de l'information;

h) mesures destinées à réduire et à résoudre les défaillances des systèmes d'information qui entraîneraient la destruction ou la perte accidentelle, l'altération, la communication non autorisée de données à caractère personnel traitées ou l'accès non autorisé à de telles données;

i) conformité;

j) sécurité du réseau informatique (il est recommandé d'appliquer la norme ISO/CEI 27033 ou la SoGP).

L'application de ces normes peut être limitée aux parties de l'organisation qui sont pertinentes pour le système de collecte en ligne. Par exemple, la sécurité des ressources humaines peut être limitée à toute personne ayant un accès physique ou réseau au système de collecte en ligne, et la sécurité physique/environnementale peut être limitée au(x) bâtiment(s) hébergeant le système.

**Exigences fonctionnelles**

2.3. Le système de collecte en ligne consiste en une instance d'application web créée aux fins de la collecte de déclarations de soutien à une seule initiative citoyenne.

2.4. Si l'administration du système requiert des tâches distinctes, les différents niveaux de contrôle d'accès sont établis selon le principe du moindre privilège.

2.5. Les éléments accessibles au public sont bien séparés des éléments destinés à l'administration du système. Aucun contrôle d'accès n'entrave la lecture des informations disponibles dans la partie publique du système, y compris les renseignements relatifs à l'initiative et le formulaire électronique de déclaration de soutien. Il n'est possible de signer en faveur d'une initiative qu'à l'intérieur de cette partie publique.

2.6. Le système détecte et empêche la présentation de doubles déclarations de soutien.

**Sécurité de l'application**

2.7. Le système est protégé de façon appropriée contre les vulnérabilités et attaques de type «exploits» connus. À cette fin, il satisfait, entre autres, aux exigences énoncées ci-après.

2.7.1. Le système est protégé contre les failles d'injection telles que les requêtes SQL (langage d'interrogation structuré), les requêtes LDAP (*Lightweight Directory Access Protocol*), les requêtes en langage XML Path (XPath), les commandes du système d'exploitation ou les arguments du programme. Les exigences minimales à respecter à cet effet sont les suivantes:

a) Toute la saisie utilisateur est validée.

b) La validation est effectuée au moins par la logique côté serveur.

c) Toute utilisation d'interpréteurs repose sur une distinction claire entre, d'une part, les données non fiables et, d'autre part, la commande ou la requête. Pour les appels SQL, cela nécessite d'utiliser des *bind variables* dans l'ensemble des instructions élaborées et des procédures stockées, et d'éviter les requêtes dynamiques.

2.7.2. Le système est protégé contre le script de site à site (*Cross-Site Scripting* ou XSS). Les exigences minimales à respecter à cet effet sont les suivantes:

a) La sécurité de toute la saisie utilisateur renvoyée au navigateur est confirmée (par validation de la saisie).

b) Toute la saisie utilisateur fait l'objet d'une séquence d'échappement correcte avant d'être reprise dans la page de sortie.

c) Un encodage de sortie adapté fait en sorte que cette saisie est toujours considérée comme du texte dans le navigateur. Aucun contenu actif n'est utilisé.

2.7.3. Le système fait l'objet d'une gestion rigoureuse des sessions et des authentifications, ce qui impose le respect des exigences minimales suivantes:

a) Les informations d'identification sont toujours protégées au moment du stockage, par hachage ou cryptage. Le risque qu'une personne s'authentifie au moyen d'une attaque *pass-the-hash* est réduit.

b) Les informations d'identification ne peuvent pas être devinées ni écrasées en raison de faiblesses dans les fonctions de gestion de compte (par exemple, création de compte, modification du mot de passe, récupération du mot de passe, faiblesse des identifiants de session).

c) Les identifiants de session et les données de session n'apparaissent pas dans l'adresse URL.

d) Les identifiants de session ne sont pas vulnérables aux attaques de fixation de session.

e) Les identifiants de session expirent, ce qui garantit une déconnexion des utilisateurs.

f) Les identifiants de session ne sont pas régénérés une fois que la connexion est établie.

g) Les mots de passe, les identifiants de session et autres informations d'identification sont transmis uniquement par protocole TLS (*Transport Layer Security*).

h) La partie administration du système est protégée. Si elle est protégée par une authentification à un seul facteur, le mot de passe est composé au minimum de 10 caractères, comprenant au moins une lettre, un chiffre et un caractère spécial. Il est également possible d'utiliser une authentification à deux facteurs. En cas d'utilisation exclusive d'une authentification à un seul facteur, celle-ci comprend un mécanisme de vérification en deux étapes permettant d'accéder à la partie administration du système par l'internet, où le facteur unique est renforcé par un autre moyen d'authentification tel qu'un(e) phrase secrète/code à usage unique envoyé(e) par SMS ou une chaîne de demande d'accès aléatoire, cryptée de façon asymétrique, devant être décryptée à l'aide de la clé privée des organisateurs/administrateurs, non connue du système.

2.7.4. Le système ne comporte pas de références directes non sécurisées à un objet. Les exigences minimales à respecter à cet effet sont les suivantes:

a) Pour les références directes à des ressources restreintes, l'application vérifie que l'utilisateur est autorisé à accéder à la ressource précisément demandée.

b) Si la référence est indirecte, l'association vers la référence directe est limité aux valeurs autorisées pour l'utilisateur en cours.

2.7.5. Le système est protégé contre la falsification de requête intersite.

2.7.6. Une configuration de sécurité adéquate est en place, ce qui impose le respect des exigences minimales suivantes:

a) Tous les composants logiciels sont à jour, y compris le système d'exploitation, le serveur web/d'applications, le système de gestion des bases de données, les applications et toutes les bibliothèques de codes.

b) Les services non nécessaires du système d'exploitation et du serveur web/d'applications sont désactivés ou supprimés ou ne sont pas installés.

c) Les mots de passe par défaut des comptes sont modifiés ou désactivés.

d) Une gestion des erreurs est mise en place pour éviter la divulgation d'informations sensibles via les traces de la pile et d'autres messages d'erreur trop informatifs.

e) Les paramètres de sécurité dans les cadres de développement et les bibliothèques sont configurés conformément aux meilleures pratiques, telles que les directives de l'OWASP.

2.7.7. Pour le cryptage des données, le système prévoit ce qui suit:

a) Les données à caractère personnel en format électronique sont cryptées au moment où elles sont stockées ou transférées aux autorités compétentes des États membres conformément à l'article 8, paragraphe 1, du règlement (UE) nº 211/2011, les clés étant gérées et sauvegardées séparément.

b) Des algorithmes standard forts et des clés fortes sont utilisés, conformément aux normes internationales. Une gestion de clés est en place.

c) Les mots de passe sont hachés au moyen d'un algorithme standard fort et un «salt» approprié est utilisé.

d) L'ensemble des clés et des mots de passe est protégé contre les accès non autorisés.

2.7.8. Le système restreint l'accès aux URL en fonction des niveaux d'accès et des autorisations des utilisateurs. Les exigences minimales à respecter à cet effet sont les suivantes:

a) Si les contrôles d'authentification et d'autorisation pour l'accès aux pages sont assurés au moyen de mécanismes de sécurité externe, ces derniers doivent être correctement configurés pour chaque page.

b) Si une protection au niveau du code est utilisée, celle-ci doit être en place pour chaque page demandée.

2.7.9. La protection de la couche transport est suffisante. À cette fin, l'ensemble des mesures énoncées ci-dessous ou des mesures d'une efficacité au moins égale sont en place.

a) Le système requiert la version la plus récente du protocole de transfert hypertexte sécurisé (HTTPS) pour accéder à toute ressource sensible au moyen de certificats qui sont valables, non expirés, non révoqués, et correspondent à tous les domaines utilisés par le site.

b) Le système met un drapeau «sécurisé» (*secure flag*) sur tous les cookies sensibles.

c) Le serveur configure le protocole TLS de manière à n'utiliser que les algorithmes de cryptage conformes aux meilleures pratiques. Les utilisateurs sont informés qu'ils doivent activer la prise en charge TLS dans leur navigateur.

2.7.10. Le système est protégé contre les redirections et les renvois invalidés.

**Sécurité des bases de données et intégrité des données**

2.8. Lorsque les systèmes de collecte en ligne utilisés pour différentes initiatives citoyennes partagent des ressources en termes de matériel et de système d'exploitation, ils ne partagent aucune donnée, en ce compris les informations d'accès/de cryptage. En outre, l'évaluation des risques et les contre-mesures mises en place font apparaître ce partage.

2.9. Le risque qu'une personne s'authentifie à la base de données au moyen d'une attaque *pass-the-hash* est réduit.

2.10. Les données fournies par les signataires ne sont accessibles qu'à l'administrateur de la base de données/l'organisateur.

2.11. Les informations d'identification administratives, les données à caractère personnel recueillies auprès des signataires et leur sauvegarde sont sécurisées au moyen d'algorithmes de cryptage forts, conformément au point 2.7.7 b). Toutefois, l'État membre dans lequel la déclaration de soutien sera comptabilisée, la date de présentation de la déclaration de soutien et la langue dans laquelle le signataire a rempli le formulaire de déclaration de soutien peuvent être stockés dans le système sans cryptage.

2.12. Les signataires n'ont accès qu'aux données soumises au cours de la session pendant laquelle ils remplissent le formulaire de déclaration de soutien. Une fois que le formulaire de déclaration de soutien a été envoyé, la session en question est clôturée et les données transmises ne sont plus accessibles.

2.13. Les données à caractère personnel des signataires, sauvegarde comprise, ne sont disponibles dans le système qu'en format crypté. Aux fins de la consultation ou de la certification des données par les autorités nationales en application de l'article 8 du règlement (UE) n° 211/2011, les organisateurs peuvent exporter les données cryptées conformément au point 2.7.7 a).

2.14. La persistance des données introduites dans le formulaire de déclaration de soutien est atomique. En d'autres termes, une fois que l'utilisateur a encodé toutes les informations demandées dans le formulaire de déclaration de soutien et valide sa décision de soutenir l'initiative, le système valide avec succès toutes les données de ce formulaire dans la base de données ou, en cas d'erreur, ne sauve aucune donnée du tout. Le système informe l'utilisateur de la réussite ou de l'échec de sa requête.

2.15. Le système de gestion des bases de données est à jour et corrigé en permanence en fonction des nouveaux «exploits» découverts.

2.16. Tous les journaux d'activité du système sont en place. Le système est conçu de telle sorte que les journaux d'audit enregistrant les exceptions et les autres événements importants pour la sécurité énumérés ci-dessous puissent être générés et conservés jusqu'à ce que les données soient détruites conformément à l'article 12, paragraphe 3 ou 5, du règlement (UE) n° 211/2011. Les journaux sont protégés de manière adéquate, par exemple par stockage sur des supports cryptés. Les organisateurs/administrateurs contrôlent régulièrement les journaux afin de détecter toute activité suspecte. Le contenu minimal des journaux est le suivant:

a) les dates et heures d'ouverture et de fermeture de session par les organisateurs/administrateurs;

b) les sauvegardes effectuées;

c) l'ensemble des modifications et des mises à jour réalisées par les administrateurs des bases de données.

**Sécurité de l'infrastructure – emplacement physique, infrastructure réseau et environnement du serveur**

2.17. *Sécurité physique*

Quel que soit le type d'hébergement utilisé, la machine qui héberge l'application est correctement protégée, ce qui nécessite:

a) un contrôle de l'accès à la zone d'hébergement et un journal d'audit;

b) la protection physique des données de sauvegarde contre le vol ou le déplacement accidentel;

c) l'installation du serveur hébergeant l'application sur un rack sécurisé.

2.18. *Sécurité du réseau*

2.18.1. Le système est hébergé sur un serveur internet installé en zone démilitarisée (DMZ) et protégé par un pare-feu.

2.18.2. Lorsque des mises à jour et correctifs valables du produit pare-feu deviennent publics, ces mises à jour ou correctifs sont installés de manière opportune.

2.18.3. Tout le trafic entrant et sortant du serveur (destiné au système de collecte en ligne) est inspecté par les règles de pare-feu et journalisé. Les règles de pare-feu refusent tout trafic non nécessaire à la sécurité d'utilisation et d'administration du système.

2.18.4. Le système de collecte en ligne doit être hébergé sur un segment correctement protégé du réseau de production, séparé des segments utilisés pour héberger les systèmes non productifs tels que les environnements de développement ou d'essai.

2.18.5. Le réseau local (LAN) fait l'objet des mesures de sécurité suivantes:

a) liste d'accès couche 2/sécurité du commutateur de port;

b) les ports de commutateur non utilisés sont désactivés;

c) la DMZ est située sur un réseau local virtuel (VLAN)/LAN;

d) le mode *trunk* (agrégation de liaisons) au niveau de la couche 2 n'est pas activé sur les ports inutiles.

2.19. *Sécurité du système d'exploitation et du serveur web/d'applications*

2.19.1. Une configuration de sécurité adéquate, comprenant les éléments énumérés au point 2.7.6, est en place.

2.19.2. Les applications tournent avec le plus faible ensemble de privilèges nécessaire à leur exécution.

2.19.3. L'accès des administrateurs à l'interface de gestion du système de collecte en ligne est soumis à un délai d'expiration de session de courte durée (maximum 15 minutes).

2.19.4. Lorsque des mises à jour et correctifs valables du système d'exploitation, des moteurs d'exécution des applications, des applications tournant sur les serveurs ou du logiciel antiprogramme malveillant deviennent publics, ces mises à jour ou correctifs sont installés de manière opportune.

2.19.5. Le risque qu'une personne s'authentifie sur le système au moyen d'une attaque *pass-the-hash* est réduit.

2.20. *Sécurité des clients organisateurs*

Pour garantir la sécurité de bout en bout, les organisateurs prennent les mesures nécessaires pour sécuriser l'application cliente/le périphérique client qu'ils utilisent pour gérer le système de collecte en ligne et y accéder, comme suit:

2.20.1. Les utilisateurs exécutent les tâches ne relevant pas de la maintenance (tâches de bureautique, par exemple) avec le plus faible ensemble de privilèges nécessaire à cette exécution.

2.20.2. Lorsque des mises à jour et correctifs valables du système d'exploitation, de toute application installée ou du logiciel antiprogramme malveillant deviennent publics, ces mises à jour ou correctifs sont installés de manière opportune.

3. SPÉCIFICATIONS TECHNIQUES VISANT À METTRE EN ŒUVRE L'ARTICLE 6, PARAGRAPHE 4, POINT c), DU RÈGLEMENT (UE) N° 211/2011

3.1. Le système donne la possibilité d'extraire, pour chaque État membre, un rapport répertoriant l'initiative et les données à caractère personnel des signataires soumises à vérification par l'autorité compétente dudit État membre.

3.2. L'exportation des déclarations de soutien des signataires est possible sous la forme présentée à l'annexe III du règlement (UE) no 211/2011. Le système permet, en outre, l'exportation des déclarations de soutien dans un format interopérable tel que le langage XML (*Extensible Markup Language*).

3.3. Les déclarations de soutien exportées sont revêtues d'une mention indiquant qu'elles sont à *diffusion limitée* vers l'État membre concerné, et classées comme *données à caractère personnel*.

3.4. La transmission électronique des données exportées vers les États membres est protégée contre l'écoute clandestine au moyen d'un cryptage de bout en bout approprié.