II

(Rechtsakte ohne Gesetzescharakter)

VERORDNUNGEN

DURCHFÜHRUNGSVERORDNUNG (EU) Nr. 1179/2011 DER KOMMISSION

vom 17. November 2011

zur Festlegung der technischen Spezifikationen für Online-Sammelsysteme gemäß der Verordnung (EU) Nr. 211/2011 des Europäischen Parlaments und des Rates über die Bürgerinitiative

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) Nr. 211/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 über die Bürgerinitiative [1], insbesondere auf Artikel 6 Absatz 5,

nach Stellungnahme des Europäischen Datenschutzbeauftragten,

in Erwägung nachstehender Gründe:

(1) Nach der Verordnung (EU) Nr. 211/2011 müssen Online-Sammelsysteme für Unterstützungsbekundungen bestimmte Sicherheitsanforderungen und technische Vorgaben erfüllen und von der zuständigen Behörde des betreffenden Mitgliedstaats bescheinigt werden.

(2) Ein Online-Sammelsystem im Sinne der Verordnung (EU) Nr. 211/2011 ist ein Informationssystem mit Software, Hardware, Beherbergungs-/Betriebsumgebung, Geschäftsprozessen und Betriebspersonal für die Online-Sammlung von Unterstützungsbekundungen.

(3) In der Verordnung (EU) Nr. 211/2011 sind die Anforderungen festgelegt, die Online-Sammelsysteme erfüllen müssen, bevor eine Bescheinigung erteilt werden kann; darin heißt es außerdem, dass die Kommission technische Spezifikationen dafür festlegen solle.

(4) Das Dokument Top 10 2010 des OWASP-Projekts (Open Web Application Security Project) gibt einen Überblick über die größten Sicherheitsrisiken bei Webanwendungen sowie über Tools für die Risikoabwehr. Die technischen Spezifikationen bauen daher auf den Ergebnissen dieses Projekts auf.

(5) Die Einhaltung der technischen Spezifikationen durch die Organisatoren sollte garantieren, dass die Behörden der Mitgliedstaaten Online-Sammelsysteme bescheinigen, und dazu beitragen, dass alle geeigneten technischen und organisatorischen Maßnahmen ergriffen werden, um den Bestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates [2] zur Sicherheit der Verarbeitung sowohl bei der Entwicklung des Verarbeitungssystems als auch bei der Verarbeitung selbst zu entsprechen, wodurch die Sicherheit gewährleistet und somit jede unrechtmäßige Verarbeitung verhindert und personenbezogene Daten gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Offenlegung oder den unberechtigten Zugang geschützt werden sollen.

(6) Die Bescheinigung sollte dadurch erleichtert werden, dass die Organisatoren die Software verwenden, die die Kommission nach Artikel 6 Absatz 2 der Verordnung (EU) Nr. 211/2011 zur Verfügung stellt.

(7) Zur Gewährleistung des Schutzes personenbezogener Daten sollten sich die Organisatoren von Bürgerinitiativen in ihrer Funktion als die für die Verarbeitung Verantwortlichen bei der Online-Sammlung von Unterstützungsbekundungen an die technischen Spezifikationen halten, die in der vorliegenden Verordnung festgelegt sind. Wird ein Auftragsverarbeiter mit der Verarbeitung betraut, so sollten die Organisatoren sicherstellen, dass sich dieser an ihre Anweisungen und an die technischen Spezifikationen dieser Verordnung hält.

(8) Diese Verordnung wahrt die Grundrechte und beachtet die Grundsätze, die in der Charta der Grundrechte der Europäischen Union verankert sind, insbesondere in Artikel 8, wonach jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat.

(9) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des mit Artikel 20 der Verordnung (EU) Nr. 211/2011 eingesetzten Ausschusses —

[1] ABl. L 65 vom 11.3.2011, S. 1.

[2] ABl. L 281 vom 23.11.1995, S. 31.

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Die in Artikel 6 Absatz 5 der Verordnung (EU) Nr. 211/2011 vorgesehenen technischen Spezifikationen sind im Anhang festgelegt.

Artikel 2

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 17. November 2011

Für die Kommission
Der Präsident
José Manuel BARROSO

ANHANG

1. TECHNISCHE SPEZIFIKATIONEN FÜR DIE UMSETZUNG VON ARTIKEL 6 ABSATZ 4 BUCHSTABE a DER VERORDNUNG (EU) Nr. 211/2011

Um die automatische Einreichung eines Formulars für eine Unterstützungsbekundung über das System zu verhindern, wird der Unterzeichner bei der Einreichung einer solchen Unterstützungsbekundung durch ein geeignetes, der gängigen Praxis entsprechendes Verfahren überprüft. Eine Möglichkeit der Überprüfung wäre beispielsweise die Eingabe eines starken CAPTCHAs.

2. TECHNISCHE SPEZIFIKATIONEN FÜR DIE UMSETZUNG VON ARTIKEL 6 ABSATZ 4 BUCHSTABE b DER VERORDNUNG (EU) Nr. 211/2011

Normen zur Informationssicherheit

2.1. Wenn die Organisatoren nicht über eine entsprechende Zertifizierung verfügen, legen sie Unterlagen vor, aus denen hervorgeht, dass sie die Anforderungen der Norm ISO/IEC 27001 erfüllen, ohne dass sie die Norm förmlich übernehmen müssen. Zu diesem Zweck haben sie:

a) eine vollständige Risikobewertung durchgeführt, die die folgenden Aspekte abdeckt: Ermittlung des Systemumfangs; Herausstellung der Geschäftsauswirkungen im Falle verschiedener Verstöße im Bereich der Informationssicherheit; Auflistung der Bedrohungen für das Informationssystem sowie von dessen Schwachstellen; Erstellung einer Dokumentation zur Risikoanalyse, in der neben Gegenmaßnahmen, mit denen Bedrohungen entgegengewirkt werden kann, auch Abhilfemaßnahmen im Falle einer akuten Bedrohung aufgeführt sind; Aufstellung einer nach Prioritäten geordnete Liste mit Verbesserungsvorschlägen;

b) Maßnahmen zur Bewältigung von Risiken im Zusammenhang mit dem Schutz personenbezogener Daten und des Privat- und Familienlebens sowie Maßnahmen, die im Falle einer solchen Gefährdung zur Anwendung kommen, erarbeitet und umgesetzt;

c) die Restrisiken schriftlich festgehalten;

d) die organisatorischen Voraussetzungen für den Erhalt von Rückmeldungen zu neuen Bedrohungen und zu Verbesserungen im Bereich der Informationssicherheit geschaffen.

2.2. Die von den Organisatoren auf der Grundlage der Risikobewertung gemäß vorstehendem Punkt 2.1 Buchstabe a gewählten Sicherheitskontrollen entsprechen den folgenden Normen:

1. ISO/IEC 27002 oder

2. dem „Standard of Good Practice" (SoGP) des Information Security Forum (ISF).

Vorgenommen beziehungsweise geprüft werden:

a) Risikobewertungen (empfohlen wird eine Bewertung nach der Norm ISO/IEC 27005 oder eine andere für diesen Zweck geeignete Risikobewertungsmethode);

b) physische und umgebungsbezogene Sicherheit;

c) Personalsicherheit;

d) Betriebs- und Kommunikationsmanagement;

e) Standard-Zugangskontrollmaßnahmen neben den in dieser Durchführungsverordnung genannten Maßnahmen;

f) Beschaffung, Entwicklung und Wartung von Informationssystemen;

g) Umgang mit Informationssicherheitsvorfällen;

h) Maßnahmen zur Minderung bzw. Behebung von Sicherheitsverstößen im Bereich der Informationssysteme, die die Zerstörung, den zufälligen Verlust, die Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang zu den verarbeiteten personenbezogenen Daten zur Folge hätten;

i) Einhaltung von Vorgaben (Compliance);

j) Netzwerksicherheit (empfohlen werden die Norm ISO/IEC 27033 oder die SoGP).

Die Anwendung dieser Normen kann auf die Teile der Organisation beschränkt sein, die für das Online-Sammelsystem relevant sind. Die Personalsicherheit beispielsweise kann auf die Mitarbeiter begrenzt werden, die physischen oder Netzwerkzugang zum Online-Sammelsystem haben. Der Aspekt der physischen und umgebungsbezogenen Sicherheit wiederum kann auf die Gebäude beschränkt sein, in denen die systemrelevante Hard- und Software untergebracht ist.

Funktionale Anforderungen

2.3. Das Online-Sammelsystem besteht aus einer webgestützten Anwendungsinstanz und dient der Sammlung von Unterstützungsbekundungen für eine bestimmte Bürgerinitiative.

2.4. Wenn für die Verwaltung des Systems unterschiedliche Rollen erforderlich sind, werden nach dem Least-Privilege-Prinzip (so wenig Rechte wie möglich) verschiedene Ebenen der Zugangskontrolle eingerichtet.

2.5. Die öffentlich zugänglichen Funktionen sind klar von den für Verwaltungszwecke vorgesehenen Funktionen abgegrenzt. Für den Zugriff auf die im öffentlich zugänglichen Bereich des Systems enthaltenen Informationen, einschließlich Informationen zur Bürgerinitiative und zum elektronischen Formular für die Unterstützungsbekundung, wird keine Zugangskontrolle eingerichtet. Die Unterzeichnung zur Unterstützung einer Initiative ist nur über diesen öffentlichen Bereich möglich.

2.6. Das System ist in der Lage, die doppelte Einreichung von Formularen für die Unterstützungsbekundung zu erkennen und zu verhindern.

Sicherheit auf Anwendungsebene

2.7. Das System ist ausreichend gegen alle bekannten Schwachstellen und Sicherheitslücken abgesichert. In diesem Zusammenhang werden unter anderem die folgenden Anforderungen erfüllt:

2.7.1. Das System ist gegen Einschleusungen (sogenannte „Injections“) geschützt, also Schwachstellen, die es einem Angreifer erlauben, mittels SQL-Querys (Structured Query Language), LDAP-Querys (Lightweight Directory Access Protocol), XPath-Querys (XML Path Language), Betriebssystembefehlen oder Programmargumenten Befehle in die Anwendung einzuschleusen. Zu diesem Zweck müssen mindestens die folgenden Anforderungen erfüllt sein:

a) Alle Benutzereingaben werden überprüft.

b) Diese Überprüfung erfolgt mindestens über die serverseitige Logik.

c) Durch die Verwendung von Interpretern werden alle nicht vertrauenswürdigen Daten vom Befehl oder der Query getrennt. Bei SQL-Aufrufen bedeutet dies, dass in allen vorbereiteten Anweisungen (Prepared Statements) und gespeicherten Prozeduren (Stored Procedures) Bind-Variablen verwendet und dynamische Querys vermieden werden.

2.7.2. Das System ist gegen seitenübergreifendes Scripting (Cross-Site Scripting, XSS) geschützt. Zu diesem Zweck müssen mindestens die folgenden Anforderungen erfüllt sein:

a) Alle vom Benutzer gemachten Eingaben, die an den Browser zurückgesendet werden, werden auf ihre Sicherheit überprüft (per Eingabegültigkeitsprüfung).

b) Alle Benutzereingaben werden korrekt codiert, bevor sie auf der Ausgabeseite angezeigt werden.

c) Durch die korrekte Codierung der Ausgabe ist sichergestellt, dass diese Eingaben im Browser immer als Text behandelt werden. Es werden keine aktiven Inhalte verwendet.

2.7.3. Das System verfügt über leistungsstarke Authentifizierungs- und Sitzungsmanagement-Funktionen, für die mindestens die folgenden Anforderungen erfüllt sein müssen:

a) Die Anmeldedaten werden bei der Speicherung immer per Streuspeicherung („Hashing“) oder Verschlüsselung geschützt. Das Risiko, dass ein Angreifer per Hash-Übergabe („Pass-the-Hash“) auf das System zugreift, wird so verringert.

b) Die Anmeldedaten können nicht aufgrund unzureichender Kontoverwaltungsfunktionen erraten oder überschrieben werden (z. B. Anlegen von Konten, Ändern des Kennworts, Anfordern des Kennworts, Identifikatoren für unzureichend geschützte Sitzungen (Sitzungs-IDs)).

c) IDs und Daten zu einer Browsersitzung (Session) werden nicht in der URL (Uniform Resource Locator) angezeigt.

d) Sitzungs-IDs sind gegen Session-Fixation-Angriffe geschützt.

e) Sitzungs-IDs laufen ab, wodurch sichergestellt ist, dass Benutzer abgemeldet werden.

f) Sitzungs-IDs werden nach der erfolgreichen Anmeldung nicht wiederverwendet.

g) Kennwörter, Sitzungs-IDs und andere Anmeldedaten werden ausschließlich über das TLS-Verschlüsselungsprotokoll (Transport Layer Security) gesendet.

h) Der verwaltungsbezogene Teil des Systems ist geschützt. Wenn der Schutz in einer Einzelfaktor-Authentifizierung (Single-factor Authentication, SFA) besteht, muss das Kennwort mindestens 10 Zeichen, davon mindestens einen Buchstaben, eine Zahl und ein Sonderzeichen, enthalten. Alternativ kann auch die Zwei-Faktoren-Authentifizierung verwendet werden. Wenn lediglich die Einzelfaktoren-Authentifizierung zum Einsatz kommt, wird der Zugang zum verwaltungsbezogenen Teil des Systems über das Internet durch einen zweistufigen Prüfmechanismus ergänzt, wobei der Einzelfaktor durch eine zusätzliche Authentifizierungsmethode erweitert wird, beispielsweise einen per SMS zugestellten einmaligen Zugangscode bzw. -begriff oder eine asymmetrisch verschlüsselte, zufällige Zeichenkette (Challenge String), die nur über einen Schlüssel des Organisators oder Administrators entschlüsselt werden kann, der dem System nicht bekannt ist.

2.7.4. Das System enthält keine unsicheren, direkten Objektverweise. Zu diesem Zweck müssen mindestens die folgenden Anforderungen erfüllt sein:

a) Bei direkten Verweisen auf eingeschränkte Quellen prüft die Anwendung, ob der Benutzer berechtigt ist, auf die angeforderte Quelle zuzugreifen.

b) Bei einem indirekten Verweis auf eine Quelle ist das Mapping des direkten Verweises auf Werte beschränkt, die für den aktuellen Benutzer freigegeben sind.

2.7.5. Das System ist gegen die seitenübergreifende Aufruf-Manipulation (Cross-Site Request Forgery, XSRF) geschützt.

2.7.6. Es besteht eine ausreichende Sicherheitskonfiguration, wobei mindestens die folgenden Anforderungen erfüllt sein müssen:

a) Alle Softwarekomponenten, einschließlich des Betriebssystems, des Webservers und des Anwendungsservers, des Datenbank-Management-Systems (DBMS), der Anwendungen und aller Code-Bibliotheken, sind auf dem aktuellen Stand.

b) Unnötige Dienste des Betriebssystems sowie des Web- und des Anwendungsservers werden deaktiviert, entfernt oder nicht installiert.

c) Standardmäßig generierte Kennwörter werden geändert oder deaktiviert.

d) Zur Verhinderung von Sicherheitslücken durch Stack Traces und andere übermäßig detaillierte Fehlermeldungen wird ein Verfahren zur Fehlerbehandlung eingerichtet.

e) Die Sicherheitseinstellungen in den Development Frameworks und Bibliotheken werden in Übereinstimmung mit bewährten Verfahren konfiguriert, beispielsweise den Leitlinien des *Open Web Application Security Project* (OWASP).

2.7.7. Das System ermöglicht die Verschlüsselung von Daten auf folgende Weise:

a) Personenbezogene Daten in elektronischer Form werden bei der Speicherung oder der Übermittlung an die entsprechenden zuständigen Behörden in den Mitgliedstaaten gemäß Artikel 8 Absatz 1 der Verordnung (EU) Nr. 211/2011 verschlüsselt; die hierfür verwendeten Schlüssel werden in einem separaten System gesichert und verwaltet.

b) Im Einklang mit internationalen Normen werden leistungsstarke Standardalgorithmen und Schlüssel verwendet. Ein Schlüsselmanagement-System wurde eingerichtet.

c) Kennwörter werden über leistungsstarke Standardalgorithmen gehasht, und es kommt ein angemessener Salt zur Verwendung.

d) Alle Schlüssel und Kennwörter sind vor unberechtigtem Zugriff geschützt.

2.7.8. Das System schränkt den URL-Zugriff auf der Grundlage von Zugriffsebenen und Berechtigungen der Benutzer ein. Zu diesem Zweck müssen mindestens die folgenden Anforderungen erfüllt sein:

a) Wenn für die Bereitstellung von Authentifizierungs- und Berechtigungsprüfungen für den Seitenzugriff externe Sicherheitsmechanismen verwendet werden, müssen diese für jede Seite korrekt konfiguriert werden.

b) Wenn ein Sicherheitsmechanismus auf Code-Ebene verwendet wird, muss dieser für jede erforderliche Seite eingerichtet sein.

2.7.9. Das System nutzt ausreichende Schutzfunktionen auf der Transportschicht. Zu diesem Zweck müssen die folgenden oder mindestens gleichwertige Maßnahmen getroffen werden:

a) Für den Zugriff auf sensible Daten über gültige Zertifikate, die weder abgelaufen noch gesperrt sein dürfen und für alle von der Site verwendeten Domains gelten müssen, muss die neueste Version des HTTPS-Protokolls (Hypertext Transfer Protocol Secure) verwendet werden.

b) Das System setzt das Secure-Attribut für alle Cookies mit sensiblen Daten.

c) Der Server konfiguriert den TLS-Provider so, dass nur Verschlüsselungsalgorithmen unterstützt werden, die im Einklang mit bewährten Verfahren stehen. Den Benutzern wird mitgeteilt, dass sie die TLS-Unterstützung in ihren Browsern aktivieren müssen.

2.7.10. Das System ist gegen ungeprüfte Redirects und Forwards geschützt.

Datenbanksicherheit und Datenintegrität

2.8. Online-Sammelsysteme, die für verschiedene Bürgerinitiativen herangezogen werden und dieselbe Hardware und dieselben Betriebssystemressourcen nutzen, tauschen jedoch keine Daten, wie Zugriffs- und Verschlüsselungsdaten, aus. Dies spiegelt sich auch in der Risikobewertung und in den umgesetzten Gegenmaßnahmen wider.

2.9. Das Risiko, dass ein Angreifer per Hash-Übergabe auf die Datenbank zugreift, wird verringert.

2.10. Die von den Unterzeichnern vorgelegten Daten können nur vom Datenbankadministrator und vom Organisator eingesehen werden.

2.11. Administrative Benutzerinformationen, von den Unterzeichnern erhobene personenbezogene Daten sowie deren Sicherung werden mit Hilfe leistungsstarker Verschlüsselungsalgorithmen gemäß Punkt 2.7.7 Buchstabe b gesichert. Der Mitgliedstaat, dem die Unterstützungsbekundung zugerechnet wird, das Datum der Einreichung der Unterstützungsbekundung sowie die Sprache, in der der Unterzeichner das Formular für die Unterstützungsbekundung ausgefüllt hat, können hingegen unverschlüsselt im System gespeichert werden.

2.12. Die Unterzeichner haben nur Zugang zu den Daten, die in der Sitzung übermittelt wurden, in der sie auch das Formular für die Unterstützungsbekundung ausgefüllt haben. Sobald das Formular für die Unterstützungsbekundung eingereicht wurde, wird die Sitzung geschlossen, und die übermittelten Daten können nicht mehr aufgerufen werden.

2.13. Die personenbezogenen Daten der Unterzeichner, einschließlich der Datensicherung, liegen im System nur in verschlüsselter Form vor. Zum Zwecke der Einsicht und Bescheinigung der Daten durch die nationalen Behörden gemäß Artikel 8 der Verordnung (EU) Nr. 211/2011 können die Organisatoren die verschlüsselten Daten im Einklang mit Punkt 2.7.7 Buchstabe a exportieren.

2.14. Die Daten im Formular für die Unterstützungsbekundung werden atomar persistent erfasst, sind also nicht weiter zerlegbar. Wenn also ein Benutzer im Formular für die Unterstützungsbekundung alle erforderlichen Angaben gemacht hat und seine Entscheidung, die Initiative zu unterstützen, bekräftigt, schreibt das System entweder alle Formulardaten in die Datenbank oder bricht im Falle eines Fehlers ab und speichert keine Daten. Das System informiert den Benutzer darüber, ob der Vorgang erfolgreich war.

2.15. Das verwendete DBMS ist auf dem aktuellen Stand und wird laufend über Patches gegen neu ermittelte Sicherheitslücken abgesichert.

2.16. Alle Systemaktivitäten werden protokolliert. Das System stellt sicher, dass die Prüfprotokolle, in denen Ausnahmen und andere sicherheitsrelevante Ereignisse aufgeführt werden, erstellt und so lange gespeichert werden, bis die betreffenden Daten gemäß Artikel 12 Absatz 3 bzw. 5 der Verordnung (EU) Nr. 211/2011 vernichtet werden. Die Protokolle sind angemessen geschützt, beispielsweise durch die Speicherung auf verschlüsselten Medien. Die Organisatoren bzw. Administratoren überprüfen die Protokolle regelmäßig auf verdächtige Aktivitäten. Die Protokolle sollten mindestens die folgenden Informationen enthalten:

a) An- und Abmeldedaten und -zeitpunkte der Organisatoren und Administratoren;

b) Sicherungskopien;

c) vom Datenbankadministrator vorgenommene Änderungen und Aktualisierungen.

Sicherheit der Infrastruktur — physischer Ort, Netzwerkinfrastruktur und Serverumgebung

2.17. *Physische Sicherheit*

Unabhängig vom verwendeten Hostingtyp ist der Rechner, auf dem die Anwendung läuft, angemessen geschützt. Dieser Schutz umfasst Folgendes:

a) Zugangskontrolle zum Hosting-Bereich und Prüfprotokoll;

b) physischer Schutz der Sicherungsdaten vor Diebstahl und zufälligem Datenverlust;

c) Unterbringung des Servers, auf dem die Anwendung läuft, in einem abgesicherten Serverschrank.

2.18. *Netzwerksicherheit*

2.18.1. Das System läuft auf einem mit dem Internet verbundenen und durch eine Firewall geschützten Server in einer demilitarisierten Zone (DMZ).

2.18.2. Wenn relevante Updates und Patches für die verwendete Firewall zur Verfügung stehen, werden diese baldmöglichst installiert.

2.18.3. Der gesamte eingehende und ausgehende Datenverkehr zwischen dem Server und dem Online-Sammelsystem wird gemäß den Firewall-Regeln überprüft und protokolliert. Die Firewall-Regeln unterbinden jeden Datenverkehr, der nicht für die sichere Verwendung und Verwaltung des Systems relevant ist.

2.18.4. Das Online-Sammelsystem muss in einem angemessen geschützten Produktivnetzwerksegment untergebracht sein, das von den Segmenten getrennt ist, die für nicht produktive Systeme, wie Entwicklungs- oder Testumgebungen, verwendet werden.

2.18.5. Sicherheitsvorkehrungen in Bezug auf das Local Area Network (LAN) wie die Folgenden wurden eingerichtet:

a) Layer 2 (L2)-Zugriffsliste/Port-Switch-Sicherheit;

b) nicht verwendete Switchports werden deaktiviert;

c) die DMZ befindet sich in einem dedizierten VLAN (Virtual Local Area Network) bzw. LAN;

d) an unnötigen Ports ist keine L2-Bündelung (Trunking) möglich.

2.19. *Sicherheit des Betriebssystems sowie des Web- und des Anwendungsservers*

2.19.1. Es besteht eine ausreichende Sicherheitskonfiguration einschließlich der unter Punkt 2.7.6 aufgeführten Komponenten.

2.19.2. Anwendungen werden mit möglichst eingeschränkten Berechtigungen ausgeführt.

2.19.3. Für den Administratorzugriff auf die Verwaltungsoberfläche des Online-Sammelsystems ist eine kurze Sitzungshöchstdauer (max. 15 Minuten) festgelegt.

2.19.4. Wenn relevante Updates und Patches für das Betriebssystem, die Anwendungslaufzeiten oder die auf dem Server ausgeführten Anwendungen bzw. Softwareanwendungen zum Schutz vor Malware zur Verfügung stehen, werden diese Updates und Patches baldmöglichst installiert.

2.19.5. Das Risiko, dass ein Angreifer per Hash-Übergabe auf die Datenbank zugreift, wird verringert.

2.20. *Client-Sicherheit beim Organisator*

Der durchgängigen Sicherheit willen ergreifen die Organisatoren die erforderlichen Maßnahmen zum Schutz ihrer Client-Anwendungen und -Geräte, die sie beim Zugang zum Online-Sammelsystem und dessen Verwaltung anwenden. Dies umfasst beispielsweise die folgenden Maßnahmen:

2.20.1. Die Benutzer führen nicht mit Wartungsmaßnahmen verbundene Aufgaben (z. B: Büroautomatisierungsaufgaben) mit möglichst eingeschränkten Berechtigungen aus.

2.20.2. Wenn relevante Updates und Patches für das Betriebssystem oder eine beliebige installierte Anwendung bzw. Softwareanwendungen zum Schutz vor Malware zur Verfügung stehen, werden diese Updates und Patches baldmöglichst installiert.

3. TECHNISCHE SPEZIFIKATIONEN FÜR DIE UMSETZUNG VON ARTIKEL 6 ABSATZ 4 BUCHSTABE c DER VERORDNUNG (EU) Nr. 211/2011

3.1. Das System bietet die Möglichkeit, für jeden einzelnen Mitgliedstaat einen Bericht mit der Bezeichnung der Bürgerinitiative sowie den personenbezogenen Daten der Unterzeichner zu extrahieren, damit diese Angaben von der entsprechenden zuständigen Behörde dieses Mitgliedstaats überprüft werden können.

3.2. Die von den Unterzeichnern eingereichten Unterstützungsbekundungen können in dem in Anhang III der Verordnung (EU) Nr. 211/2011 enthaltenen Format exportiert werden. Darüber hinaus kann auch der Export von Unterstützungsbekundungen in einem interoperablen Format wie der Extensible Markup Language (XML) im System vorgesehen werden.

3.3. Die exportierten Unterstützungsbekundungen werden für den betreffenden Mitgliedstaat als *Verschlusssache* gekennzeichnet und mit dem Vermerk *personenbezogene* Daten versehen.

3.4. Durch eine durchgängige Verschlüsselung sind die exportierten Daten bei der elektronischen Übermittlung an die Mitgliedstaaten abhörsicher geschützt.