II

(Rechtsakte ohne Gesetzescharakter)

VERORDNUNGEN

DURCHFÜHRUNGSVERORDNUNG (EU) 2019/1799 DER KOMMISSION

vom 22. Oktober 2019

zur Festlegung der technischen Spezifikationen für individuelle Online-Sammelsysteme gemäß der Verordnung (EU) 2019/788 des Europäischen Parlaments und des Rates über die Europäische Bürgerinitiative

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2019/788 des Europäischen Parlaments und des Rates vom 17. April 2019 über die Europäische Bürgerinitiative ([1]), insbesondere auf Artikel 11 Absatz 5,

in Erwägung nachstehender Gründe:

(1) Die Verordnung (EU) 2019/788 enthält überarbeitete Vorschriften für die Europäische Bürgerinitiative und hebt die Verordnung (EU) Nr. 211/2011 des Europäischen Parlaments und des Rates ([2]) auf.

(2) Gemäß der Verordnung (EU) 2019/788 müssen Organisatoren bei der Online-Sammlung von Unterstützungsbekundungen für registrierte Bürgerinitiativen das zentrale Online-Sammelsystem nutzen, das von der Kommission eingerichtet und betrieben wird. Um jedoch die Übergangsphase für die Initiativen zu erleichtern, die noch vor Ende 2022 gemäß der Verordnung (EU) 2019/788 registriert werden, können sich die Organisatoren entscheiden, ihr eigenes individuelles Online-Sammelsystem zu nutzen.

(3) Nach der Verordnung (EU) 2019/788 sollte ein individuelles System, das für die Online-Sammlung von Unterstützungsbekundungen genutzt wird, über hinreichende Sicherheits- und sonstige technische Merkmale verfügen, um zu gewährleisten, dass die Daten während der gesamten Sammlungsfrist sicher gesammelt, gespeichert und übermittelt werden. Die Kommission sollte gemeinsam mit den Mitgliedstaaten die technischen Spezifikationen für die Umsetzung der Anforderungen an individuelle Online-Sammelsysteme festlegen.

(4) Die Bestimmungen dieser Verordnung ersetzen die in der Durchführungsverordnung (EU) Nr. 1179/2011 der Kommission ([3]) festgelegten Regeln, die daher hinfällig werden.

(5) Die durchzuführenden technischen und organisatorischen Maßnahmen sollten sowohl zum Zeitpunkt der Systementwicklung als auch während der gesamten Sammlungsfrist jede unbefugte Verarbeitung personenbezogener Daten verhindern und sie gegen die zufällige oder unrechtmäßige Vernichtung, den zufälligen Verlust, die Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang schützen.

([1]) ABl. L 130 vom 17.5.2019, S. 55.
([2]) Verordnung (EU) Nr. 211/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 über die Bürgerinitiative (ABl. L 65 vom 11.3.2011, S. 1).
([3]) 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 (ABl. L 301 vom 18.11.2011, S. 3).

(6) Zu diesem Zweck sollten die Organisatoren angemessene Risikomanagementverfahren anwenden, um die Risiken für ihre Systeme zu ermitteln und geeignete und verhältnismäßige Gegenmaßnahmen festzulegen, um diese Risiken auf ein vertretbares Maß zu reduzieren. Die Organisatoren sollten die ermittelten Risiken für die Sicherheit und den Datenschutz sowie die Maßnahmen zur Vermeidung dieser Risiken unter Berücksichtigung der von der Bescheinigungsbehörde angewandten Sicherheitsanforderungen und -vorschriften ordnungsgemäß dokumentieren. Die Sicherheitsanforderungen und -vorschriften sollten mit der Verordnung (EU) 2019/788 in Einklang stehen und auf Anfrage von der Bescheinigungsbehörde bereitgestellt werden.

(7) Die Umsetzung der in dieser Verordnung festgelegten technischen Spezifikationen sollte unbeschadet der Verpflichtung der Organisatoren gelten, die gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([4]) geltenden Datenschutzanforderungen zu erfüllen, einschließlich der etwaigen Notwendigkeit einer Datenschutz-Folgenabschätzung.

(8) Der Vertreter einer Organisatorengruppe oder gegebenenfalls einer juristischen Person im Sinne von Artikel 5 Absatz 7 der Verordnung (EU) 2019/788 gilt in Bezug auf die Verarbeitung personenbezogener Daten in einem individuellen Online-Sammelsystem als für die Verarbeitung Verantwortlicher im Sinne der Verordnung (EU) 2016/679.

(9) Organisatoren, die Änderungen ihres individuellen Online-Sammelsystems nach der Zertifizierung des Systems vornehmen, sollten die jeweilige Bescheinigungsbehörde unverzüglich darüber in Kenntnis setzen, wenn die Änderung die der Zertifizierung zugrunde liegende Bewertung beeinflussen könnte. Vorher können die Organisatoren die Stellungnahme der Bescheinigungsbehörde einholen, um zu überprüfen, ob die Änderung solche Auswirkungen haben kann und daher gemeldet werden sollte.

(10) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([5]) angehört und hat am 16. September 2019 eine Stellungnahme abgegeben. Die Europäische Agentur für Netz- und Informationssicherheit wurde konsultiert und übermittelte ihre Anmerkungen am 18. Juli 2019.

(11) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des nach Artikel 22 der Verordnung (EU) 2019/788 eingesetzten Ausschusses —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Die in Artikel 11 Absatz 5 der Verordnung (EU) 2019/788 genannten technischen Spezifikationen sind im Anhang der vorliegenden Verordnung festgelegt.

Artikel 2

(1) Die Organisatoren stellen sicher, dass ihr individuelles Online-Sammelsystem während der gesamten Sammlungsfrist die im Anhang aufgeführten technischen Spezifikationen erfüllt.

(2) Die Organisatoren setzen die nach Artikel 11 Absatz 3 der Verordnung (EU) 2019/788 zuständige Behörde des Mitgliedstaats unverzüglich über Änderungen, die nach der Zertifizierung des Systems durch diese bescheinigende Behörde im System oder in den unterstützenden organisatorischen Maßnahmen vorgenommen wurden, in Kenntnis, wenn diese Änderungen die der Zertifizierung zugrunde liegende Bewertung beeinflussen könnten. Vorher können die Organisatoren die Stellungnahme der zuständigen Behörde einholen, um zu überprüfen, ob die Änderung solche Auswirkungen haben kann.

([4]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

([5]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

Artikel 3

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

Sie gilt ab dem 1. Januar 2020.

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

Brüssel, den 22. Oktober 2019

Für die Kommission
Der Präsident
Jean-Claude JUNCKER

ANHANG

1. **TECHNISCHE SPEZIFIKATIONEN FÜR DIE UMSETZUNG VON ARTIKEL 11 ABSATZ 4 BUCHSTABE A DER VERORDNUNG (EU) 2019/788**

Das System umfasst technische Maßnahmen, die sicherstellen, dass nur natürliche Personen Unterstützungsbekundungen abgeben können. Mit den technischen Maßnahmen dürfen nicht mehr personenbezogene Daten gesammelt und gespeichert werden als die in Anhang III zur Verordnung (EU) 2019/788 aufgeführten.

2. **TECHNISCHE SPEZIFIKATIONEN FÜR DIE UMSETZUNG VON ARTIKEL 11 ABSATZ 4 BUCHSTABE B DER VERORDNUNG (EU) 2019/788**

Die Organisatoren treffen angemessene und wirksame technische und organisatorische Maßnahmen zur Eindämmung der Risiken für die Sicherheit der von ihnen eingesetzten Netz- und Informationssysteme, um sicherzustellen, dass die Informationen über die Initiative, die im Online-Sammelsystem bereitgestellt und der Öffentlichkeit im Internet zugänglich gemacht werden, den im Register nach Artikel 6 Absatz 5 der Verordnung (EU) 2019/788 veröffentlichten Informationen über die Initiative entsprechen.

Die Organisatoren stellen sicher, dass

a) die Informationen, die im Online-Sammelsystem über die Initiative bereitgestellt werden, den im Register veröffentlichten Informationen entsprechen;

b) das System die im Register veröffentlichten Informationen über die Initiative anzeigt, bevor die Bürger die Unterstützungsbekundungen abgeben;

c) Sicherheitsmaßnahmen eingeführt wurden, die gewährleisten, dass die Dateneingabefelder in den Unterstützungsbekundungen zusammen mit den Informationen über die betreffende Initiative angezeigt werden, damit das Risiko vermieden wird, dass Unterstützungsbekundungen durch eine falsche Darstellung der Initiative für eine andere Initiative abgegeben werden;

d) das System die Daten nach der Abgabe der Unterstützungsbekundung zusammen mit den Informationen über die Initiative speichert;

e) Sicherheitsmaßnahmen dafür sorgen, dass an den im Online-Sammelsystem bereitgestellten Informationen über die Initiative keine unbefugten Änderungen vorgenommen werden können.

3. **TECHNISCHE SPEZIFIKATIONEN FÜR DIE UMSETZUNG VON ARTIKEL 11 ABSATZ 4 BUCHSTABE C DER VERORDNUNG (EU) 2019/788**

Mit dem System wird gewährleistet, dass die Unterstützungsbekundungen in Übereinstimmung mit den in Anhang III der Verordnung (EU) 2019/788 vorgesehenen Datenfeldern abgegeben werden.

Mit dem System wird gewährleistet, dass eine Person eine Unterstützungsbekundung nur dann abgeben kann, wenn sie bestätigt hat, dass sie die in Anhang III der Verordnung (EU) 2019/788 festgelegte Datenschutzerklärung gelesen hat.

4. **TECHNISCHE SPEZIFIKATIONEN FÜR DIE UMSETZUNG VON ARTIKEL 11 ABSATZ 4 BUCHSTABE D DER VERORDNUNG (EU) 2019/788**

4.1. **Verwaltung**

4.1.1. Die Organisatorengruppe ernennt einen Sicherheitsbeauftragten, der für die Sicherheit des Systems und die sichere Übermittlung der gesammelten Unterstützungsbekundungen an die zuständige Behörde des verantwortlichen Mitgliedstaats verantwortlich ist. Der Sicherheitsbeauftragte überwacht die Informationssicherung sowie die technischen und organisatorischen Sicherheitsmaßnahmen für die sichere Sammlung, Speicherung und Übermittlung der von den Unterzeichnern bereitgestellten Daten.

4.1.2. Die Organisatoren können die nationale zuständige Behörde nach Artikel 11 Absatz 3 der Verordnung (EU) 2019/788 auffordern, die für die Zertifizierung individueller Online-Sammelsysteme anwendbaren Sicherheitsvorschriften und -anforderungen bereitzustellen. Die zuständige Behörde stellt die Sicherheitsvorschriften und -anforderungen in der Regel innerhalb eines Monats nach Eingang des Antrags bereit. Die anwendbaren Sicherheitsvorschriften und -anforderungen müssen mit den einschlägigen nationalen oder internationalen Sicherheitsstandards in Einklang stehen.

4.1.3. In den für die Zertifizierung des Systems anwendbaren Sicherheitsvorschriften und -anforderungen werden die in Abschnitt 4.2 definierten Risiken und die Spezifikationen in Abschnitt 4.3 berücksichtigt.

4.2. **Informationssicherung**

4.2.1. Die Organisatoren wenden Risikomanagementverfahren an, um die Risiken im Zusammenhang mit der Nutzung ihrer Systeme, einschließlich in Bezug auf die Rechte und Freiheiten der Unterzeichner, zu ermitteln und geeignete und verhältnismäßige Maßnahmen festzulegen, um Vorfälle, die die Sicherheit der von ihnen verwendeten Netze und Informationssysteme beeinträchtigen könnten, zu verhindern bzw. deren Auswirkungen abzumildern.

Das Risikomanagementverfahren konzentriert sich insbesondere auf die Risiken im Zusammenhang mit der Vertraulichkeit und Integrität der Informationen im System. Diese Risiken können das Ergebnis von Bedrohungen sein wie

a) Benutzerfehler

b) Fehler der System-/Sicherheitsadministratoren

c) Konfigurationsfehler

d) Infektionen durch Malware

e) unbeabsichtigte Veränderung von Informationen

f) Offenlegung oder Weitergabe von Informationen

g) Softwareschwachstellen

h) unberechtigter Zugang

i) Abfangen oder Abhören der Datenströme

j) Datenschutzrisiken.

4.2.2. Die Organisatoren legen Unterlagen vor, aus denen hervorgeht, dass sie:

a) die Risiken des Systems bewertet haben;

b) geeignete Maßnahmen getroffen haben, um Vorfälle, die die Sicherheit des Systems beeinträchtigen könnten, zu verhindern bzw. deren Auswirkungen abzumildern;

c) die Restrisiken ermittelt haben;

d) die Maßnahmen umgesetzt und ihre Umsetzung überprüft haben;

e) die organisatorischen Voraussetzungen für den Erhalt von Informationen zu neuen Bedrohungen und zu Verbesserungen im Bereich der Informationssicherheit geschaffen haben;

f) die Zertifizierungsanforderungen gemäß Artikel 11 Absatz 4 der Verordnung (EU) 2019/788, einschließlich der dafür erforderlichen Verfahren, während des gesamten Sammlungsprozesses erfüllen.

4.2.3. Die Maßnahmen zur Verhinderung von Vorfällen, die die Sicherheit des Systems beeinträchtigen könnten, bzw. zur Abmilderung deren Auswirkungen umfassen folgende Bereiche:

a) Personalsicherheit

b) Zugangskontrolle

c) kryptografische Kontrollen

d) physische Sicherheit und umgebungsbezogene Sicherheit

e) Betriebssicherheit

f) Kommunikationssicherheit

g) Anschaffung, Entwicklung und Instandhaltung der Systeme

h) Handhabung von Informationssicherheitsvorfällen

i) Compliance.

Die Anwendung dieser Sicherheitsmaßnahmen kann auf die Teile der Organisation beschränkt werden, die für das Online-Sammelsystem relevant sind. Die Personalsicherheit beispielsweise kann auf die Mitarbeiter begrenzt werden, die physischen oder logischen Zugang 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.

4.2.4. Übertragen die Organisatoren die Entwicklung oder Bereitstellung von Online-Sammelsystemen oder Teilen davon einem Auftragsverarbeiter, so legen sie Unterlagen vor, anhand derer die Bescheinigungsbehörde feststellen kann, ob die erforderlichen Sicherheitskontrollen vorhanden sind.

4.3. **Datenverschlüsselung**

Das System sieht folgende Verschlüsselung von Daten vor:

a) Personenbezogene Daten in elektronischer Form werden bei der Speicherung oder der Übermittlung an die zuständigen Behörden in den Mitgliedstaaten gemäß der Verordnung (EU) 2019/788 verschlüsselt; die hierfür verwendeten Schlüssel werden in einem separaten System gesichert und verwaltet.

b) Es werden geeignete Standardalgorithmen und geeignete Schlüssel gemäß internationalen Standards (wie der ETSI-Norm) verwendet. Eine Schlüsselverwaltung ist vorhanden.

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