

II

(Незаконодателни актове)

РЕГЛАМЕНТИ

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2019/1799 НА КОМИСИЯТА

от 22 октомври 2019 година

относно определяне на технически спецификации за индивидуални системи за събиране на изявления за подкрепа онлайн по силата на Регламент (ЕС) 2019/788 на Европейския парламент и на Съвета относно европейската гражданска инициатива

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) 2019/788 на Европейския парламент и на Съвета от 17 април 2019 г. относно европейската гражданска инициатива ⁽¹⁾, и по-специално член 11, параграф 5 от него,

като има предвид, че:

- (1) С Регламент (ЕС) 2019/788 се определят преработени правила относно европейската гражданска инициатива и се отменя Регламент (ЕС) № 211/2011 на Европейския парламент и на Съвета ⁽²⁾.
- (2) В Регламент (ЕС) 2019/788 се предвижда, че за събирането на изявления за подкрепа онлайн за регистрирани граждански инициативи организаторите трябва да използват централната система за събиране на изявления за подкрепа онлайн, създадена и поддържана от Комисията. При все това, за да се улесни преходът, за инициативите, регистрирани по Регламент (ЕС) 2019/788 преди края на 2022 г., организаторите могат да използват своя собствена индивидуална система за събиране на изявления за подкрепа онлайн.
- (3) Съгласно Регламент (ЕС) 2019/788 индивидуалните системи, които се използват за събирането на изявления за подкрепа онлайн, следва да имат подходящи технически характеристики и характеристики за сигурност, за да се гарантират сигурното събиране, съхраняване и прехвърляне на данните по време на цялата процедура. Комисията следва да определи, заедно с държавите членки, техническите спецификации за изпълнение на изискванията за индивидуалните системи за събиране на изявления онлайн.
- (4) Правилата, установени в настоящия регламент, заменят тези, определени в Регламент за изпълнение (ЕС) № 1179/2011 на Комисията ⁽³⁾, които следователно вече няма да са актуални.
- (5) Техническите и организационните мерки, които трябва да бъдат изпълнени, следва да имат за цел да предотвратят, както в момента на разработване на системата, така и по време на периода на събиране, всяко неразрешено обработване на лични данни и да предоставят защита срещу случайно или незаконно унищожаване или случайна загуба, промяна, неразрешено разкриване или достъп.

⁽¹⁾ ОВ L 130, 17.5.2019 г., стр. 55.

⁽²⁾ Регламент (ЕС) № 211/2011 на Европейския парламент и на Съвета от 16 февруари 2011 г. относно гражданската инициатива (ОВ L 65, 11.3.2011 г., стр. 1).

⁽³⁾ Регламент за изпълнение (ЕС) № 1179/2011 на Комисията от 17 ноември 2011 г. относно определяне на технически спецификации за системите за събиране на изявления за подкрепа онлайн по силата на Регламент (ЕС) № 211/2011 на Европейския парламент и на Съвета относно гражданската инициатива (ОВ L 301, 18.11.2011 г., стр. 3).

- (6) За тази цел организаторите следва да прилагат подходящи процеси за управление на риска, за да идентифицират рисковете за своите системи и да определят подходящи и пропорционални мерки за противодействие с цел намаляване на тези рискове до приемливи нива. Организаторите следва да документират по подходящ начин установените рискове за сигурността и защитата на данните и мерките, предприети за борба с тези рискове, като се вземат предвид правилата и изискванията за сигурност, прилагани от удостоверяващия орган. Правилата и изискванията за сигурност следва да бъдат в съответствие с Регламент (ЕС) 2019/788 и следва да бъдат предоставени от удостоверяващия орган при поискване.
- (7) Техническите спецификации, определени в настоящия регламент, следва да се прилагат без да се засяга задължението на организаторите да спазват изискванията за защита на данните, произтичащи от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ⁽⁴⁾, включително евентуалната необходимост от оценка на въздействието върху защитата на данните.
- (8) Представителят на група на организаторите или, в зависимост от случая, юридическо лице, както е посочено в член 5, параграф 7 от този регламент, се считат за администратори на данни по смисъла на Регламент (ЕС) 2016/679 във връзка с обработването на лични данни в индивидуална система за събиране на изявления онлайн.
- (9) Организаторите, които въвеждат промени в своята индивидуална система за събиране на изявления онлайн, след като системата е била удостоверена, следва да уведомят без ненужно забавяне съответния удостоверяващ орган, ако тази промяна може да се отрази на оценката, която е в основата на удостоверяването. Преди това организаторите може да поискат становището на удостоверяващия орган за това дали промяната може да окаже подобно въздействие и следователно подлежи на уведомяване.
- (10) В съответствие с член 42 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ⁽⁵⁾ беше проведена консултация с Европейския надзорен орган по защита на данните, който представи становище на 16 септември 2019 г. беше проведена консултация с Агенцията на Европейския съюз за мрежова и информационна сигурност и тя представи мнение на 18 юли 2019 г.
- (11) Мерките, предвидени в настоящия регламент, са в съответствие със становището на комитета, създаден съгласно член 22 от Регламент (ЕС) 2019/788,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Техническите спецификации, посочени в член 11, параграф 5 от Регламент (ЕС) 2019/788, се определят в приложението към настоящия регламент.

Член 2

1. Организаторите гарантират, че тяхната индивидуална система за събиране на изявления за подкрепа онлайн отговаря на техническите спецификации, както са определени в приложението, през целия период на събиране.
2. Организаторите уведомяват без неоправдано забавяне компетентния орган на съответната държава членка, посочен в член 11, параграф 3 от Регламент (ЕС) 2019/788, за промените, които се въвеждат в системата или в подкрепящите организационни мерки, след като системата е била удостоверена от този орган, когато тези промени може да повлияят на оценката, на която се основава удостоверяването. Преди това организаторите могат да потърсят съвета на компетентния орган за това дали промяната може да окаже такова въздействие.

⁽⁴⁾ Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

⁽⁵⁾ Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39)

Член 3

Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Той се прилага от 1 януари 2020 г.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 22 октомври 2019 година.

За Комисията
Председател
Jean-Claude JUNCKER

ПРИЛОЖЕНИЕ

1. Технически спецификации за прилагане на член 11, параграф 4, буква а) от Регламент (ЕС) 2019/788

Системата следва да прилага технически мерки, за да се гарантира, че само физически лица могат да изпращат изявления за подкрепа. Техническите мерки не следва да изискват събирането и съхраняването на лични данни извън посочените в приложение III към Регламент (ЕС) 2019/788.

2. Технически спецификации за прилагане на член 11, параграф 4, буква б) от Регламент (ЕС) 2019/788

Организаторите следва да въведат подходящи и ефективни технически и организационни мерки за управление на рисковете за сигурността на мрежовите и информационните системи, използвани от тях при техните операции, за да се гарантира, че предоставената за инициативата информация в системата за събиране на изявления за подкрепа онлайн, както е представена онлайн на обществеността, съответства на информацията, публикувана за инициативата в регистъра, посочен в член 6, параграф 5 от Регламент (ЕС) 2019/788.

Организаторите следва да гарантират, че:

- а) информацията, предоставена за инициативата в системата за събиране на изявления онлайн, отговаря на информацията, публикувана в регистъра;
- б) системата представя информацията за инициативата, публикувана в регистъра, преди гражданинът да подаде изявлението за подкрепа;
- в) налице са мерки за сигурност, с които да се гарантира, че полетата за въвеждане на данни в изявленията за подкрепа се представят заедно с информацията за инициативата, с цел да се предотврати рискът изявления за подкрепа да се представят за различна инициатива поради невярно представяне на инициативата;
- г) системата гарантира, че след подаването на изявлението за подкрепа данните в него се запазват заедно с информацията за инициативата;
- д) налице са мерки за сигурност, с които да се предотврати предприемането на неразрешени промени в информацията, предоставена по инициативата, в системата за събиране на изявления онлайн.

3. Технически спецификации за прилагане на член 11, параграф 4, буква в) от Регламент (ЕС) 2019/788

Системата следва да гарантира, че изявленията за подкрепа се представят в съответствие с полетата за данни в приложение III към Регламент (ЕС) 2019/788.

Системата следва да гарантира, че дадено лице може да представи изявление за подкрепа, само след като потвърди, че е прочело декларацията за поверителност в приложение III към Регламент (ЕС) 2019/788.

4. Технически спецификации за прилагане на член 11, параграф 4, буква г) от Регламент (ЕС) 2019/788**4.1. Управление**

4.1.1. Групата на организаторите следва да определи служител по сигурността, който отговаря за сигурността на системата и сигурното предаване на събраните изявления за подкрепа на компетентния орган на отговорната държава членка. Служителят по сигурността следва да извършва надзор над процесите за осигуреност на информацията и техническите и организационните мерки за сигурност, за да се гарантират сигурното събиране, съхранение и предаване на данните, предоставени от поддръжниците.

4.1.2. Организаторите могат да поискат от националния компетентен орган, посочен в член 11, параграф 3 от Регламент (ЕС) 2019/788, да предостави приложимите правила и изисквания за сигурност за удостоверяването на индивидуални системи за събиране на изявления онлайн. Компетентният орган предоставя правилата и изискванията за сигурност като правило в срок от един месец след получаване на искането. Приложимите правила и изисквания за сигурност следва да бъдат в съответствие със съществуващите подходящи национални или международни стандарти за сигурност.

4.1.3. Правилата и изискванията за сигурност за удостоверяването на системата следва да са насочени към противодействие на рисковете, определени в раздел 4.2, и да отчитат спецификациите в раздел 4.3.

4.2. Осигуреност на информацията

4.2.1. Организаторите следва да използват процеси за управление на риска с цел да идентифицират рисковете, свързани с използването на техните системи, включително за правата и свободите на поддръжниците, и за определяне на подходящите и пропорционалните мерки за предотвратяване и смекчаване на въздействието на инциденти, засягащи сигурността на мрежовите и информационните системи, които използват в своите операции.

Процесът за управление на риска следва да се съсредоточава основно върху рисковете, свързани с поверителността и целостта на информацията, съдържаща се в системата. Тези рискове могат да произтичат от заплахи, включително:

- а) грешки на потребителя;
- б) системни грешки или грешки на администратора по сигурността;
- в) грешки в конфигурацията;
- г) заразяване с опасен софтуер;
- д) неволно променяне на информация;
- е) оповестяване или изтичане на информация;
- ж) уязвими елементи в софтуера;
- з) непозволен достъп;
- и) прихващане и подслушване на трафика от данни;
- й) рискове за защитата на данните.

4.2.2. Организаторите следва да предоставят документи, доказващи, че те:

- а) са направили оценка на рисковете за системата;
- б) са определили подходящи мерки за предотвратяване и смекчаване на въздействието на инциденти, засягащи сигурността на системата;
- в) са идентифицирали остатъчните рискове;
- г) са приложили мерките и проверяват тяхното изпълнение;
- д) са предвидили от организационна гледна точка начини за получаване на обратна информация за нови заплахи и подобрения на сигурността;
- е) изпълняват през целия процес на събиране на данни изискванията във връзка с удостоверяването, предвидени в член 11, параграф 4 от Регламент (ЕС) 2019/788, включително разполагат с необходимите процеси, за да гарантират това.

4.2.3. Мерките за предотвратяване и смекчаване на въздействието на инциденти, засягащи сигурността на системите, обхващат следните области:

- а) сигурност на човешките ресурси;
- б) контрол на достъпа;
- в) криптографски контрол;
- г) физическа сигурност и сигурност на средата;
- д) сигурност на операциите;
- е) сигурност на комуникациите;
- ж) придобиване, разработка и поддръжка на системи;
- з) управление на инциденти, свързани със сигурността на информацията;
- и) съответствие.

Прилагането на тези мерки за сигурност може да бъде ограничено до тези части на организацията, които са от значение за системата за събиране на изявления за подкрепа онлайн. Така например сигурността на човешките ресурси може да бъде ограничена до персонала, който има физически достъп или мрежови достъп до системата за събиране на изявления за подкрепа онлайн, а физическата сигурност и сигурността на средата могат да бъдат ограничени до сградата(ите), в която(ито) се помещава системата.

4.2.4. Когато организаторите са възложили разработването или внедряването на системите за събиране на изявления онлайн или на части от тях, организаторите предоставят на удостоверяващия орган документи, за да може той да докаже, че е налице необходимият контрол на сигурността.

4.3. Криптиране на данни

Системата следва да дава възможност за следното криптиране на данни:

- а) личните данни в електронен формат се криптират при съхраняване или прехвърляне до компетентните органи на държавите членки в съответствие с Регламент (ЕС) 2019/788, като ключовете се управляват и запазват отделно;
 - б) подходящи стандартни алгоритми и подходящи ключове следва да се използват в съответствие с международните стандарти (като например стандарта на ETSI). следва да е налице управление на ключовете;
 - в) всички ключове и пароли следва да са защитени срещу неразрешен достъп.
-