Становище на Комитета (член 64)

Становище 28/2022 относно критериите за сертифициране Europrivacy във връзка с тяхното одобряване от ЕКЗД като Европейски печат за защита на данните в съответствие с член 42, параграф 5 от ОРЗД

Прието на 10 октомври 2022 г.

Европейският комитет по защита на данните,

като взе предвид член 63, член 64, параграф 2 и член 42 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година 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 (наричан по-нататък „ОРЗД“),

като взе предвид Споразумението за Европейското икономическо пространство (наричано по-нататък „ЕИП“), и по-специално приложение XI и протокол 37 към него, изменени с Решение на Съвместния комитет на ЕИП № 154/2018 от 6 юли 2018 г.[1],

като взе предвид членове 10 и 22 от своя Правилник за дейността,

(1) Държавите членки, надзорните органи, Европейският комитет по защита на данните (наричан по-нататък „ЕКЗД“ или „Комитетът“) и Европейската комисия насърчават, особено на равнището на Съюза, създаването на механизми за сертифициране за защита на данните (наричани по-нататък „механизми за сертифициране“) и на печати и маркировки за защита на данните с цел да се демонстрира спазването на ОРЗД при операциите по обработване от страна на администраторите и обработващите лични данни, като се отчитат конкретните нужди на микропредприятията, на малките и средните предприятия[2]. Освен това въвеждането на механизми за сертифициране може да увеличи прозрачността и да позволи на субектите на данни да оценяват нивото на защита на данните на съответните продукти и услуги[3].

(2) Критериите за сертифициране са неразделна част от един механизъм за сертифициране. Следователно, ОРЗД изисква критериите за националния механизъм за сертифициране да бъдат одобрявани от компетентния надзорен орган (член 42, параграф 5 и член 43, параграф 2, буква б) от ОРЗД) или в случая на Европейски печат за защита на данните — от ЕКЗД (член 42, параграф 5 и член 70, параграф 1, буква о) от ОРЗД).

(3) Когато надзорен орган (наричан по-нататък „НО“) възнамерява да предложи Европейски печат за защита на данните за одобряване от ЕКЗД в съответствие с член 42, параграф 5 от ОРЗД, НО следва да заяви намерението на собственика на схемата да предлага механизма за сертифициране във всички държави членки. В този случай основната роля на ЕКЗД е да гарантира съгласуваното прилагане на ОРЗД посредством механизма за съгласуваност, посочен в членове 63, 64 и 65 от ОРЗД. В тази връзка, ЕКЗД одобрява критериите за сертифициране съгласно член 64, параграф 2 от ОРЗД.

(4) Целта на настоящото становище е да се гарантира съгласуваното прилагане на ОРЗД, включително от страна на надзорните органи, администраторите и обработващите лични данни, с оглед на основните елементи, които трябва да бъдат разработени от механизмите за сертифициране. По-специално, оценката на ЕКЗД се извършва въз основа на „Насоки 1/2018 относно сертифицирането и определянето на критериите за сертифициране в съответствие с членове 42 и 43 от Регламента“ (наричани по-нататък „Насоките“) и допълнението към тях, в

[1] Позоваванията на „държави членки“ в настоящото становище следва да се разбират като позовавания на „държавите — членки на ЕИП“.
[2] Член 42, параграф 1 от ОРЗД.
[3] Съображение 100 от ОРЗД.

което се предоставят „Насоки относно оценяване на критериите за сертифициране“ (наричано по-нататък „Допълнението“), чийто период за обществена консултация изтече на 26 май 2021 г.

(5) В съответствие с това ЕКЗД признава, че всеки механизъм за сертифициране следва да се разглежда отделно и не засяга оценяването на който и да е друг механизъм за сертифициране.

(6) Механизмите за сертифициране следва да дават възможност на администраторите и обработващите лични данни да демонстрират съответствие с ОРЗД. Следователно, техните критерии следва да отразяват надлежно предвидените в ОРЗД изисквания и принципи в областта на защитата на личните данни и да допринасят за неговото съгласувано прилагане.

(7) Същевременно собственикът на схемата следва да гарантира синхронизирането и съответствието на механизма за сертифициране с евентуални включени или използвани ISO стандарти и практики в областта на сертифицирането.

(8) Вследствие на това, сертифицирането следва да има добавена стойност за администраторите и обработващите лични данни, като помага за внедряване на стандартизирани и конкретизирани организационни и технически мерки, които доказуемо улесняват и укрепват спазването на ОРЗД при операциите по обработване, като се вземат под внимание специфичните за всеки сектор изисквания.

(9) ЕКЗД приветства усилията, положени от собствениците на схеми за разработване на механизми за сертифициране, които представляват практични и потенциално ефективни, от гледна точка на разходите, инструменти за гарантиране на по-голяма съгласуваност с ОРЗД и насърчаване на правото на неприкосновеност на личния живот и защита на данните на субектите на данни посредством повишаване на прозрачността.

(10) ЕКЗД припомня, че сертифицирането е доброволен инструмент за отчетност и че придържането към механизъм за сертифициране не намалява отговорността на администраторите или обработващите лични данни за спазването на ОРЗД, нито възпрепятства надзорните органи да изпълняват задачите и правомощията си в съответствие с ОРЗД и съответното национално законодателство.

(11) В настоящото становище ЕКЗД разглежда въпроси като обхвата, приложимостта и относимостта на критериите във всички държави членки.

(12) Настоящото становище е съсредоточено върху критериите за сертифициране. В случай че ЕКЗД изисква информация на високо равнище относно методите на оценяване, за да може задълбочено да прецени възможността за оценка на критериите в рамките на своето становище, в него не се включва никакво одобрение на посочените методи на оценяване.

(13) Становището на ЕКЗД се приема съгласно член 64, параграф 2 от ОРЗД във връзка с член 10, параграф 2 от Правилника за дейността на Европейския комитет по защита на данните в рамките на осем седмици от първия работен ден, след като председателят и компетентният надзорен орган са взели решение, че досието е пълно. По решение на председателя този срок може да бъде удължен с още шест седмици поради сложното естество на въпроса. Ако в становището ЕКЗД извежда заключението, че критериите не може да бъдат одобрени в настоящото им състояние, НО може да подаде отново критериите за одобряване, когато бъдат отстранени притесненията, изразени в първоначалното становище на ЕКЗД.

ПРИЕ СЛЕДНОТО СТАНОВИЩЕ:

КРАТКО ИЗЛОЖЕНИЕ НА ФАКТИТЕ

1. В съответствие с член 42, параграф 5 от ОРЗД и с Насоките, критериите Europrivacy v.60 (наричани по-нататък „проектът на критерии за сертифициране“, „критериите за сертифициране“ или „критериите“) са изготвени от Европейският център за сертифициране и поверителност (наричан по-нататък „собственикът на схемата“).

2. Надзорният орган на Люксембург (наричан по-нататък „НО на Люксембург“) е представил критериите за сертифициране Europrivacy за одобряване от ЕКЗД в съответствие с член 64, параграф 2 от ОРЗД на 28 септември 2022 г. Решението относно пълнотата на досието е взето на 28 септември 2022 г.

3. Механизмът за сертифициране Europrivacy не е сертифициране съгласно член 46, параграф 2, буква е) от ОРЗД, предназначено за международно предаване на лични данни, и следователно не предоставя подходящите гаранции в рамките на предаването на лични данни към трети държави или международни организации при условията, посочени в член 46, параграф 2, буква е). Всъщност всяко предаване на лични данни към трета държава или международна организация трябва да се осъществява само ако са спазени разпоредбите на глава V от ОРЗД.

2 ОЦЕНКА

4. ЕКЗД проведе оценката си на критериите за сертифициране с оглед тяхното одобряване съгласно член 42, параграф 5 от ОРЗД в съответствие със структурата, предвидена в приложение 2 към Насоките (наричано по-нататък „приложението“) и допълнението към тях.

5. ЕКЗД отбелязва, че предоставените от собственика на схемата насоки за изпълнение и предложени средства за проверка в механизма за сертифициране невинаги са съгласувани в целия каталог от критерии. Например в раздел Т.2.3.2 се изисква да са налице правила, политики, процедури или механизми за засичане и сигнализиране за прониквания (например система за засичане на прониквания, която следи мрежовия трафик за подозрителна дейност и сигнализира, когато бъде открита такава дейност), докато в предложените средства за проверка се прави позоваване на инспекция и тест за проникване (които се изискват съгласно раздел Т.2.3.1). Въпреки че подобни несъответствия не попадат в обхвата на оценката му, ЕКЗД подчертава, че те може да са пречка за акредитацията на сертифициращия орган, освен ако не бъдат отстранени от собственика на схемата.

2.1 Обхват на механизма за сертифициране и обект на оценката (ОнО)

6. Механизмът за сертифициране Europrivacy е обща схема, доколкото е насочена към голям набор от различни операции по обработване, извършвани от администратори и обработващи лични данни от най-различни сектори на дейност. Основните критерии на този механизъм за сертифициране се състоят от „Core criteria“ (Главни критерии) и „TOMs checks and controls“ (Проверки и контрол по линия на техническите и организационните мерки), които се отнасят до технологичните и организационните мерки, въведени с цел обезпечаване на сигурността на обработваните лични данни. Наборът от критерии в „Проверки и контрол по линия на

техническите и организационните мерки“ се прилага само ако обектът на оценката (наричан по-нататък „ОнО“) обработва специални категории данни, данни, свързани с престъпления, или лични данни на дете.

7. Освен това критериите включват и „Complementary contextual checks and controls“ (Допълнителни проверки на съдържанието и контрол), които имат за цел да гарантират, че осъществяваното в ОнО обработване на данни спазва специфичните изисквания за съответната сфера и технологии. Собственикът на схемата е представил информативна матрица, в която се описва спрямо кои категории операции по обработване на данни се прилага всеки набор от критерии в раздела „Допълнителни проверки на съдържанието и контрол“.

8. ЕКЗД приветства общите схеми, в които са включени специфични критерии, за да може те да са измерими и приложими спрямо специфични операции по обработване или сектор на дейност. ЕКЗД иска обаче да поясни също така, че в рамките на една обща схема не се изисква да се преценява пълнотата на критериите, свързани със специфични операции по обработване, поради което тя не е оценена в настоящото становище. Освен това ЕКЗД припомня, че когато той публикува документи, свързани с конкретни дейности по обработване, те трябва да бъдат взети под внимание от собственика на схемата и акредитираните сертифициращи органи.

9. Критериите, приложими спрямо спецификацията на ОнО, са определени в изискванията, представени в A.2.1.1. Конкретните правила, приложими спрямо процеса, който ще бъде следван от заявителя и от сертифициращия орган с оглед определяне на ОнО, са посочени в схемата Europrivacy (10.2 — Pre-certification Activities (Дейности преди сертифицирането)).

10. Комитетът отбелязва, че съгласно предоставената от НО на Люксембург документация, свързана с обхвата на механизма за сертифициране, схемата Europrivacy се прилага спрямо администратори и обработващи лични данни, установени в Европейския съюз (ЕС) или в Европейското икономическо пространство (ЕИП). Приложимостта на критериите се определя в зависимост от ролята и отговорностите на заявителя.

11. Комитетът отбелязва, че администратор на данни може да предложи за одобрение в рамите на процеса по сертифициране на Europrivacy, обект на оценка който е предмет на съвместно администриране на данни (критерии в A.2.7.1). В случай че ОнО е предмет на съвместно администриране на данни, Комитетът подчертава, че акредитираният сертифициращ орган ще трябва да проведе внимателно процедурата по кандидатстване, за да гарантира, че ОнО е от значение и че заявителят носи пълната отговорност за съответствието с всички задължения съгласно ОРЗД, които механизмът за сертифициране има за цел да демонстрира. Следователно, договорността, сключена между заявителя и останалите съвместни администратори, участващи в ОнО, с която се уреждат съответните им отговорности за спазване на задълженията съгласно ОРЗД[4], може да попречи на заявителя да изпълни критериите за сертифициране, в зависимост от същността на дейностите по обработване на ОНО.

[4] *Определянето на съответните им отговорности трябва по-специално да се отнася до упражняването на правата на субектите на данни и задълженията за предоставяне на информация. Освен това разпределението на отговорностите следва да обхваща и други задължения на администратора, например свързаните с общите принципи за защита на данните, правното основание, мерките за сигурност, задължението за уведомяване за нарушения на сигурността на данните, оценките на въздействието върху защитата на данните, използването на обработващи лични данни, предаването на данни на трети държави и комуникирането със субектите на данни и*

12. Комитетът отбелязва, че обработването на генетични данни е изключено от обхвата на механизма за сертифициране Europrivacy. Следователно в проведената от Комитета оценка на критериите не е обхванатa пригодността на критериите за ОнО, който би включвал обработване на такива данни.

2.2 Операции по обработване

13. В критериите се обхващат съответните компоненти на операциите по обработване (данни, системи и обработване), които имат отношение към общия обхват на механизма за сертифициране. По-специално критериите позволяват идентифицирането на специални категории данни, както са определени в член 9 от ОРЗД (раздел G.2 от критериите — Special Data Processing (Обработване на специални данни)).

2.3 Законосъобразност на обработването

14. Съгласно критериите се изисква проверка на законосъобразността на обработването на данните за всяка отделна операция по обработване в ОнО и на изискванията за правно основание, както са определени в член 6 от ОРЗД (раздел G.1 от критериите — Lawfulness of Data Processing (Законосъобразност на обработването на данните)).

2.4 Принципи на обработването на данни

15. В критериите се разглеждат по подходящ начин принципите за защита на данните съгласно член 5 от ОРЗД. По-специално съгласно критериите се изисква от заявителя да докаже, че личните данни са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“).

2.5 Общи задължения на администраторите и обработващите лични данни

16. В критериите се отразяват задълженията на администратора на данни в съответствие с член 24 от ОРЗД (G.4 — Data Controller Responsibility (Отговорност на администратора на данни)) и изискват оценяване на договорните отношения между обработващ лични данни и администратор в съответствие с член 28 от ОРЗД (раздел G.5 от критериите — Data Processors or sub Processors (Обработващи лични данни или подизпълнители, обработващи данни)).

17. Съгласно критериите се изисква всички заявители да назначат длъжностно лице по защита на данните (ДЛЗД) дори в случаи, в които заявителят не е задължен да определи ДЛЗД съгласно член 37 от ОРЗД. Съгласно критериите се проверява дали ДЛЗД отговаря на изискванията по членове 37—39 (раздел G.9 от критериите — Data Protection Officer (Длъжностно лице по защита на данните)).

18. Съгласно критериите се проверява съдържанието на регистрите на дейностите по обработване в съответствие с член 30 от ОРЗД (раздел G.5.3 от критериите — Records of processing activities (Регистри на дейностите по обработване)).

2.6 Права на субектите на данни

19. В критериите се разглежда по подходящ начин правото на субекта на данните да бъде информиран в съответствие с глава III от ОРЗД и се изисква въвеждането на съответни мерки.

надзорните органи (Насоки 07/2020 относно понятията „администратор“ и „обработващ лични данни“ в ОРЗД).

Съгласно критериите се изисква също така въвеждането на мерки, предвиждащи възможността за намеса в операцията по обработване с цел да се гарантират правата на субектите на данни и да се разрешава коригирането, изтриването или ограничаването (раздел G.3 от критериите — Rights of the Data Subjects (Права на субектите на данни)).

2.7 Рискове за правата и свободите

20. Съгласно критериите се изисква оценяване на риска за правата и свободите на физическите лица, свързан с обработването на данни, осъществявано в ОнО, в съответствие с член 35 от ОРЗД (раздел G.8 от критериите — Data Protection Impact Assessment (Оценка на въздействието върху защитата на данните)).

2.8 Технически и организационни мерки, гарантиращи защита

21. Съгласно критериите се изисква прилагането на технически и организационни мерки, предвиждащи поверителност, цялост и наличност на операциите по обработване. Съгласно критериите се изисква също така прилагането на технически мерки с цел внедряване на защита на данните на етапа на проектирането и по подразбиране в съответствие с членове 25 и 32 от ОРЗД (раздел G.6 от критериите — Security of Processing and Data Protection by Design (Сигурност на обработването и защита на данните на етапа на проектирането), раздел T.1/T.2 от критериите — Core Security Requirements/Extended Security Requirements (Основни изисквания за сигурност/Разширени изисквания за сигурност)).

22. Съгласно критериите се изисква прилагането на мерки за гарантиране, че задълженията за уведомяване при нарушение на сигурността на данните се изпълняват своевременно и с надлежния обхват в съответствие с членове 33 и 34 от ОРЗД (раздел G.7 от критериите — Management of Data Breaches (Управление на нарушенията на сигурността на данните)).

2.9 Критерии за доказване на съществуването на подходящи гаранции за предаването на лични данни

23. Съгласно критериите се изисква идентифициране на всички предавания на лични данни към трети държави или международни организации, които се осъществяват в ОнО, и обосноваване на направения избор, като се вземе предвид механизма за предаване на данни, осигуряващ подходящи гаранции, в съответствие с глава V от ОРЗД (раздел G.10 от критериите — Transfers of personal data to third countries or international organisations (Предавания на лични данни към трети държави или международни организации)).

3. ДОПЪЛНИТЕЛНИ КРИТЕРИИ ЗА ЕВРОПЕЙСКИ ПЕЧАТ ЗА ЗАЩИТА НА ДАННИТЕ

24. Съгласно Насоките в оценката трябва да се включи въпросът „Могат ли критериите да вземат под внимание законодателството или сценариите на държавите членки в областта на защитата на данните?“. В раздел G.1.1.3 от критериите се изисква заявителят да предостави такава оценка в доклад за оценка на съответствието с националните задължения (National Obligations Compliance Assessment Report или NOCAR). Комитетът отбелязва, че този доклад включва оценка на националните задължения, приложими спрямо ОнО, и в него ще бъдат документирани мерките, предприети от заявителя с оглед спазване на приложимите правила, и евентуално текущи коригиращи действия. Заявителят няма да използва списъка с ключовите допълващи национални изисквания, предоставен от собственика на схемата за всяка държава, като

изчерпателен списък на националните задължения, приложими спрямо ОнО. Ориентировъчният списък с минимални допълващи проверки и контрол, който се изисква да бъде предоставен от собственика на схемата, не представлява критерий за сертифициране в обхвата на настоящото становище.

ЗАКЛЮЧЕНИЯ/ПРЕПОРЪКИ

25. В заключение ЕКЗД счита, че критериите за сертифициране Europrivacy са в съответствие с ОРЗД, и ги одобрява съгласно задачата на Комитета, определена в член 70, параграф 1, буква о) от ОРЗД, което води до общо сертифициране (Европейски печат за защита на данните).

26. ЕКЗД ще регистрира механизма за сертифициране Europrivacy в публичния регистър на механизмите за сертифициране и печатите и маркировките за защита на данните в съответствие с член 42, параграф 8.

ЗАКЛЮЧИТЕЛНИ ЗАБЕЛЕЖКИ

27. Настоящото становище е предназначено за НО на Люксембург и ще бъде публикувано съгласно член 64, параграф 5, буква б) от ОРЗД.

За Европейския комитет по защита на данните

Председател