Становище на Комитета (член 64)

Становище 19/2024 относно критериите за сертифициране на EuroPrise във връзка с тяхното одобряване от Комитета като Европейски печат за защита на данните в съответствие с член 42, параграф 5 от ОРЗД

Прието на 16 юли 2024 г.

Съдържание

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 механизъма за сертифициране. Следователно, ОРЗД изисква критериите на национален 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 рамка, съгласно член 64, параграф 2 от ОРЗД, ЕКЗД одобрява критериите за сертифициране.

(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

[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.

членове 42 и 43 от Регламента“ (наричани по-нататък „Насоките“) и допълнението към тях, в 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 трябва 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 стандарти ISO, 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 специализирани организационни и технически мерки, за които е доказано, че улесняват и укрепват спазването на ОРЗД при операциите по обработване, като се вземат под внимание специфичните за всеки сектор изисквания.

(9) ЕКЗД приветства положените усилия от собствениците на схеми за разработване на механизми за сертифициране, които са практични и потенциално рентабилни 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 извърши подробна преценка на възможността за одит на критериите в рамките на своето становище, като последното не 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:

1. КРАТКО ИЗЛОЖЕНИЕ НА ФАКТИТЕ

1. В съответствие с член 42, параграф 5 от ОРЗД и Насоките проектът „Каталог на критериите на EuroPrise за сертифициране на операции по обработване на данни от страна на обработващите лични данни (обхват: ЕС) v1.5“ (наричан по-нататък „проект на критерии за сертифициране“, „критерии за сертифициране“ или „критерии“) е изготвен от EuroPriSe Cert GmbH (наричан по-нататък „собственик на схемата“), юридическо лице в Германия, и представен на Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, компетентния германски надзорен орган в Северен Рейн-Вестфалия (наричан по-нататък DE-NRW SA).

2. Германският надзорен орган (наричан по-нататък „НО на Германия“) е представил проекта за сертификационни критерии за одобряване от ЕКЗД в съответствие с член 64, параграф 2 от ОРЗД на 29 април 2024 г. Решението относно пълнотата на досието е взето на 29 май 2024 г.

3. Механизмът за сертифициране на EuroPrise 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 на трети държави или международни организации съгласно условията, посочени в член 46, параграф 2, буква е). Всъщност всяко предаване на лични данни на трета държава или международна организация трябва да се осъществява само ако са спазени разпоредбите на глава V от ОРЗД.

2. ОЦЕНКА

4. ЕКЗД извърши своята оценка на критериите за сертифициране за тяхното одобрение съгласно член 42, параграф 5 от ОРЗД в съответствие със структурата, предвидена в приложение 2 към Насоките (наричано по-долу „Приложението“) и допълнението към него.

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

5. Механизмът за сертифициране на EuroPrise съдържа критерии за сертифициране на обща за целия ЕС схема за сертифициране на обработването от обработващите лични данни. Предметът на сертификатите, за който се прилага каталогът с критерии, представлява операции по обработване, извършвани в производството на продукти, при управлението на процеси и предоставянето на услуги или с помощта на (също и няколко) продукти и услуги, по отношение на които заявителят за сертифициране действа като обработващ лични данни. Основните критерии на този механизъм за сертифициране са разделени на три набора от изисквания, а именно: от правна гледна точка (набор 1), от гледна точка на техническите и организационните мерки (набор 2) и от гледна точка на правата на субектите на данни (набор 3).

6. Заявителите за сертифициране по тази схема трябва да бъдат обработващи лични данни. Това включва обработващи лични данни, които са пряко натоварени с обработването на лични данни от администратор по смисъла на член 4, параграф 7 от ОРЗД. Заявителите за сертифициране обаче могат да бъдат и обработващи лични данни по смисъла на член 28, параграф 2 и (4) от ОРЗД (обработващи лични данни подизпълнители).

7. Когато обработващ лични данни — сертифициран по схемата за сертифициране на EuroPrise — използва подизпълнител, последният не може да твърди, че е сертифициран по схемата за сертифициране на EuroPrise. В този случай само операциите по обработване, извършвани от

първоначалния и сертифициран обработващ лични данни, са обхванати от сертифицирането. Обработващите лични данни подизпълнители обаче също могат да кандидатстват за сертифициране, което би довело до самостоятелна и независима процедура.

8. Комитетът отбелязва, че съгласно предоставената от НО на Германия документация, свързана с обхвата на механизма за сертифициране, схемата на EuroPrise се прилага спрямо обработващи лични данни, установени в Европейския съюз (ЕС) или в Европейското икономическо пространство (ЕИП).

2.2 Операции по обработване на данни

9. Обхватът на тези критерии не е ограничен до определени видове операции по обработване. Това е по-скоро методологията, на която се основава оценката на EuroPrise, която дава възможност за сертифициране на всякакви операции по обработване от страна на обработващите лични данни. Следователно, това е универсален методологичен подход, въз основа на който могат да бъдат сертифицирани голям брой много различни операции по обработване. В тази връзка е от основно значение да се спазват методологичните изисквания, тъй като това е единственият начин да се гарантира еднакво прилагане на критериите за сертифициране и съпоставимо равнище на изпитване при различните процедури за сертифициране. Целта е да се осигури сравнимост и възпроизводимост на издадените сертификати и техните резултати.

2.3 Законосъобразност и принципи на обработката на данни

10. Критериите изискват да се провери дали операциите по обработване на данни, които трябва да бъдат сертифицирани, съответстват на принципите на защита на данните на етапа на проектирането и по подразбиране (раздел 1.5 от критериите), което предполага участието на заявителя в подпомагането на администратора при прилагането на тези принципи. Това позволява да се оцени съответствието с член 25 от ОРЗД във връзка с член 5 от ОРЗД. Въпреки че няма критерии, пряко насочени към спазването на член 6 от ОРЗД — като се има предвид фактът, че администраторът носи отговорност за законосъобразността на обработването — критериите имат за цел да гарантират, че обработващите данни — заявителите проектират операциите по обработване, които да бъдат сертифицирани по начин, който улеснява прилагането от администраторите на принципите за защита на данните по член 5 от ОРЗД, включително принципа на законосъобразност на обработването.

2.4 Общи задължения на администраторите и обработващите лични данни

11. Критериите отразяват отношенията между обработващия лични данни и администратора. По-специално, критериите предвиждат задължението на обработващия лични данни да разполага с образец на споразумение за обработване на данни с администратора, който да включва всички изисквания на член 28 от ОРЗД (раздел 1.2 от критериите).

12. Критериите изискват от кандидатите да назначат длъжностно лице по защита на данните (ДЛЗД) в съответствие с член 37 от ОРЗД и да представят доказателство за назначаването на ДЛЗД (напр. удостоверение за назначаване). Съгласно критериите се проверява дали ДЛЗД отговаря на изискванията по членове 37—39 (набор 1, раздел 1.1 от критериите).

13. Съгласно критериите се проверява съдържанието на регистъра на дейностите по обработване в съответствие с член 30 от ОРЗД (набор 1, раздел 1.1 от критериите).

2.5 Права на субектите на данни

14. 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. 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 (набор 3 от критериите).

2.6 Рискове за правата и свободите

15. Според критериите се изисква обработващият лични данни да е запознат с възможните рискове за правата и свободите на физическите лица във връзка с обработването на данни, включено в ОнО. Ако има вероятност обработването на лични данни да доведе до висок риск за правата и свободите на физическите лица, няколко критерия гарантират възможността на заявителя да докаже, че изискванията на член 35 от ОРЗД са изпълнени в съответствие с член 35 от ОРЗД (раздел 1.2.2 от критериите, изискване № 6, раздел 1.3.2 от критериите, раздел 1.3.3 от критериите, раздел 2.1.5.1 от критериите, раздел 2.1.5.9 от критериите).

2.7 Технически и организационни мерки, гарантиращи защита

16. Съгласно критериите се изисква прилагането на технически и организационни мерки, предвиждащи поверителност, цялост и наличност на операциите по обработване. Критериите изискват също така прилагането на технически мерки за осигуряване на защита на данните на етапа на проектирането и по подразбиране в съответствие с член 25 и член 32 от ОРЗД (раздел 1.5 от критериите, раздел 2.1 от критериите/други документи).

17. Съгласно критериите се изисква прилагането на мерки за гарантиране, че задълженията за уведомяване при нарушение на сигурността на личните данни се изпълняват своевременно и с надлежния обхват в съответствие с членове 33 и 34 от ОРЗД (раздел 1.2.2 от критериите, изискване № 6).

2.8 Критерии с цел доказване на съществуването на подходящи гаранции за предаването на лични данни

18. Съгласно критериите се изисква идентифициране на всички предавания на лични данни на трети държави или международни организации, които участват в ОнО, и обосноваване на направения избор по отношение на механизма за предаване на данни, осигуряващ подходящи гаранции, в съответствие с глава V от ОРЗД (раздел 1.4 от критериите).

3. ДОПЪЛНИТЕЛНИ КРИТЕРИИ ЗА ЕВРОПЕЙСКИ ПЕЧАТ ЗА ЗАЩИТА НА ДАННИТЕ

19. Съгласно Насоките в оценката трябва да се включи въпросът „дали критериите са съгласувани със законодателството или сценариите на държавите членки в областта на защитата на данните?“. В раздел 4 от критериите се изисква кандидатът да спазва приложимото национално и съответното специфично за сектора законодателство за защита на данните. Освен това Комитетът разбира, че „докладът за съответствие с националното законодателство“ — в който се оценява по-специално съответствието на обекта на оценка с приложимите изисквания на националното законодателство в областта на защитата на данните — се изготвя от правни

експерти, при условие че тези експерти са доказали необходимото ниво на експертни познания в областта на приложимото национално законодателство.

ЗАКЛЮЧЕНИЯ/ПРЕПОРЪКИ

20. В заключение ЕКЗД счита, че критериите за сертифициране са в съответствие с ОРЗД, и ги одобрява съгласно задължението на Комитета, определено в член 70, параграф 1, буква о) от ОРЗД, вследствие на което е налице единно сертифициране (Европейски печат за защита на данните).

21. ЕКЗД ще регистрира каталогът на EuroPrise с критерии за сертифициране на операции по обработване на данни от обработващите лични данни в публичния регистър на механизмите за сертифициране и печатите и маркировките за защита на данните в съответствие с член 42, параграф 8.

ЗАКЛЮЧИТЕЛНИ ЗАБЕЛЕЖКИ

22. Настоящото становище е предназначено за надзорния орган на Германия в Северен Рейн-Вестфалия и ще бъде публикувано съгласно член 64, параграф 5, буква б) от ОРЗД.

За Европейския комитет по защита на данните

Председател
Anu Talus