Становище на Комитета (член 64)

Становище 14/2020 по проекторешение на компетентния надзорен орган на Ирландия относно одобрението на изискванията за акредитация на сертифициращ орган съгласно член 43, параграф 3 (ОРЗД)

Прието на 25 май 2020 г.

Прието

Съдържание

1 Обобщение на фактите 4

2 Оценка 5

2.1 Обща обосновка на ЕКЗД по внесения проект на решение 5

2.2 Основни критерии за оценка (член 43, параграф 2 от ОРЗД и Приложение 1 към Насоките на ЕКЗД), заложени в изискванията за акредитация, с оглед извършване на преценка на следните положения: 6

2.2.1 ВЪВЕДЕНИЕ (Раздел 0 от проектните изисквания за акредитация на НО на Ирландия) 7

2.2.2 ТЕРМИНИ И ОПРЕДЕЛЕНИЯ 7

2.2.3 ОБЩИ БЕЛЕЖКИ 7

2.2.4 ОСНОВНИ ИЗИСКВАНИЯ ЗА АКРЕДИТАЦИЯ (Раздел 4 от проектните изисквания за акредитация) 7

2.2.5 ИЗИСКВАНИЯ ПО ОТНОШЕНИЕ НА СТРУКТУРАТА (Раздел 5 от проектните изисквания за акредитация) 7

2.2.6 ИЗИСКВАНИЯ ПО ОТНОШЕНИЕ НА РЕСУРСИТЕ (Раздел 6 от проектните изисквания за акредитация) 8

2.2.7 ИЗИСКВАНИЯ КЪМ ПРОЦЕСИТЕ (Раздел 7 от проектните изисквания за акредитация) 8

3 Заключения/Препоръки 9

4 Заключителни забележки 9

Европейският комитет по защита на данните

като взе предвид член 63, член 64, параграф 1, буква в), параграфи 3—8 и член 43, параграф 3 от 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 (по-нататък „ОРЗД“),

като взе предвид Споразумението за Европейското икономическо пространство, и по-конкретно 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 от 25 май 2018 г.,

като има предвид, че:

1) Основната роля на Комитета е да гарантира последователното прилагане на Регламент 2016/679 (наричан по-нататък „ОРЗД“) в Европейското икономическо пространство. В съответствие с член 64, параграф 1 от ОРЗД, Комитетът издава становище, с което надзорният орган (НО) възнамерява да одобри изискванията за акредитация на сертифициращи органи съгласно член 43. Следователно, целта на настоящото становище е да създаде хармонизиран подход относно изискванията, които надзорният орган по защита на данните или националният орган по акредитация ще приложи за акредитацията на сертифициращ орган. Въпреки че ОРЗД не налага единен набор от изисквания за акредитация, чрез него се насърчава съгласуваността. Комитетът се стреми да постигне тази цел в своите становища: първо като насърчава НО да изготвят своите изисквания за акредитация като спазват структурата, заложена в Приложение 1 към Насоките 4/2018 на ЕКЗД относно акредитацията на сертифициращите органи и второ – чрез анализирането им, използвайки образец, предоставен от ЕКЗД, който позволява сравнителен анализ на изискванията (в съответствие с ISO 17065 и Насоките на ЕКЗД относно акредитацията на сертифициращи органи).

2) Позовавайки се на член 43 от ОРЗД, компетентните надзорни органи следва да приемат изискванията за акредитация. Те прилагат механизма за съгласуваност, за да може да се създаде доверие в механизма за сертифициране, в частност, като вдигнат нивото на изискванията.

3) Това, че изискванията за акредитация са предмет на механизма за съгласуваност, не означава, че следва да бъдат идентични. Компетентните надзорни органи имат свобода на преценка във връзка с националните и регионални специфики, като следва да вземат предвид местното законодателство. Целта на становището на ЕКЗД не е да постигне единен списък с изисквания на ЕС, а по-скоро да се избегнат значителни несъответствия, които може да окажат влияние, например, върху доверието в независимостта или експертния опит на акредитираните сертифициращи органи.

4) „Насоки 4/2018 относно акредитацията на сертифициращи органи съгласно член 43 от Общия регламент относно защитата на данните (2016/679)“ (по-нататък „Насоките“) и „Насоки 1/2018 относно сертифицирането и определянето на критерии за сертификация в съответствие

[1] Позоваванията на „Съюза“ в настоящото становище следва да се разбират като позовавания на „ЕИП“.

с членове 42 и 43 от Регламент 2016/679“ ще са водещи документи при прилагането на механизма за съгласуваност.

5) Ако дадена държава членка предвижда сертифициращите органи да бъдат акредитирани от надзорния орган, този орган следва да определи изисквания за акредитация, включително, но не ограничени до, изискванията, посочени в член 43, параграф 2 на ОРЗД. В сравнение със задълженията, свързани с акредитацията на сертифициращите органи от страна на националните органи по акредитация, в член 43 на ОРЗД се дава по-малко информация относно изискванията за акредитация, когато самият надзорен орган извършва акредитацията. В интерес на осигуряването на хармонизиран подход към акредитацията, прилаганите от надзорния орган изисквания за акредитация следва да са съгласно ISO/IEC 17065, като следва да се допълват от допълнителните изисквания, които надзорният орган определя в съответствие с член 43, параграф 1, буква б) от ОРЗД. ЕКЗД отбелязва, че в член 43, параграф 2, букви а)—д) от ОРЗД са отразени и конкретизирани изискванията на ISO 17065, което допринася за съгласуваността.[2]

6) Становището на ЕКЗД следва да се приеме съгласно член 64, параграф 1, буква в), параграф 3 и параграф 8 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 установили, че досието е пълно. По решение на председателя този срок може да бъде удължен с още шест седмици поради сложното естество на въпроса.

ПРИЕ СТАНОВИЩЕТО:

1 ОБОБЩЕНИЕ НА ФАКТИТЕ

1. Надзорният орган на Ирландия (по-нататък „НО на Ирландия“) внесе своите проектни изисквания за акредитация съгласно член 43, параграф 1, буква б) при ЕКЗД. Досието е прието за пълно на 13 февруари 2020 г. Националният орган по акредитация на Ирландия (INAB) ще извършва акредитация на сертифициращи органи, за да удостоверява използването на критериите за сертификация от ОРЗД. Това означава, че INAB ще прилага ISO 17065 и допълнителните изисквания, определени от НО на Ирландия, след като бъдат одобрени от същия орган, в съответствие със становището на Комитета относно проектните изисквания, за да акредитира сертифициращи органи.

2. В съответствие с член 10, параграф 2 от Правилника за дейността на Комитета, поради сложното естество на разглеждания въпрос, председателят реши да удължи първоначалния срок за приемане от осем седмици с още шест седмици.

[2] Насоки 4/2018 относно акредитацията на сертифициращите органи съгласно член 43 от Общия регламент относно защитата на данните, параграф 39. Достъпни на: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

2 ОЦЕНКА

2.1 Обща обосновка на ЕКЗД по внесения проект на решение

3. Целта на настоящото становище е да оцени изискванията за акредитация, разработени от НО, следвайки критериите, заложени в ISO 17065 или разписани като пълен списък от изисквания, с цел да се позволи на националния орган по акредитация или НО съгласно член 43, параграф 1 от ОРЗД да акредитира сертифициращ орган, отговорен за издаването и подновяването на сертификация в съответствие с член 42 от ОРЗД. Това не засяга задачите и правомощията на компетентния НО. В този конкретен случай Комитетът отбелязва, че НО на Ирландия е решил да се обърне към своя национален орган по акредитация (NAB) за издаване на акредитация, като е изпълнил допълнителните изисквания в съответствие с Насоките, които следва да се прилагат от NAB, когато издава акредитация.

4. Тази оценка на допълнителните изисквания за акредитация на НО на Ирландия цели да проучи разликите (добавяния и заличавания) към Насоките, особено Приложение 1 от тях. Освен това становището на ЕКЗД се фокусира върху всички аспекти, които могат да окажат влияние върху последователния подход, прилаган при акредитацията на сертифициращи органи.

5. Следва да се отбележи, че целта на Насоките по акредитацията на сертифициращи органи е да се окаже помощ на НО при определянето на изискванията им за акредитация. Приложението към Насоките не представлява самò по себе си изисквания за акредитация. Следователно е необходимо изискванията за акредитация на сертифициращи органи да бъдат определени от НО по начин, който позволява тяхното практическо и съгласувано приложение, както се изисква от НО.

6. Комитетът приема факта, че като се има предвид експертния им опит, на националните органи по акредитация следва да бъде дадена свобода за действие, когато определят конкретни специфични разпоредби в рамките на приложимите изисквания за акредитация. Но Комитетът счита за необходимо да изтъкне, че в случаите, когато са определени допълнителни изисквания, те следва да бъдат определени по начин, който позволява тяхното практическо, последователно приложение и преразглеждане според изискванията.

7. Комитетът отбелязва, че стандартите ISO, по-специално ISO 17065, са предмет на права на интелектуална собственост, поради което това становище няма да се позовава на текста от съответния документ. В резултат на това, Комитетът реши, когато е приложимо, да се насочи към конкретни раздели на стандарт ISO, но без да цитира текста.

8. Накрая Комитетът извърши оценката си в съответствие със структурата, предвидена в Приложение 1 към Насоките (по-нататък „Приложение“). В случаите, когато в настоящото становище няма тълкуване на конкретен раздел от проектните изисквания за акредитация на НО на Ирландия, следва да се счита, че Комитетът няма коментари и не препоръчва на НО на Ирландия да предприема последващо действие.

9. В настоящото становище не се разглеждат въпроси, посочени от НО на Ирландия, които са извън приложното поле на член 43, параграф 2 от ОРЗД, например препратки към националното законодателство. Въпреки това, Комитетът отбелязва, че националното законодателство следва да бъде в съответствие с ОРЗД, когато е необходимо.

2.2 Основни критерии за оценка (член 43, параграф 2 от ОРЗД и Приложение 1 към Насоките на ЕКЗД), заложени в изискванията за акредитация, с оглед извършване на преценка на следните положения:

1) посочване на всички ключови области, които ясно са обозначени в Приложението към Насоките, и вземане предвид на всяко отклонение от Приложението;

2) независимост на сертифициращия орган;

3) конфликти на интереси на сертифициращия орган;

4) експертен опит на сертифициращия орган;

5) подходящи гаранции, с които да се гарантира, че критериите за сертификация на ОРЗД се прилагат правилно от сертифициращия орган;

6) процедури за издаване, периодичен преглед и оттегляне на сертификация на ОРЗД; и

7) прозрачно разглеждане на жалби относно нарушения на сертификацията.

10. Като се има предвид, че:

а. В член 43, параграф 2 от ОРЗД се съдържа списък с области на акредитация, които сертифициращият орган трябва да предвиди, за да бъде акредитиран.

б. В член 43, параграф 3 от ОРЗД е предвидено, че изискванията за акредитация на сертифициращи органи се одобряват от компетентния надзорен орган.

в. В член 57, параграф 1, букви п) и р) от ОРЗД е предвидено, че компетентен надзорен орган трябва да изготвя проект на изисквания за акредитация на сертифициращи органи и да ги публикува, както и че може да провежда сам акредитацията на сертифициращите органи.

г. В член 64, параграф 1, буква в) от ОРЗД е предвидено, че Комитетът трябва да издаде становище, когато надзорният орган възнамерява да приеме изискванията за акредитация за сертифициращ орган съгласно член 43, параграф 3.

д. Ако акредитацията се извършва от националния орган по акредитация в съответствие с ISO/IEC 17065/2012, трябва да се прилагат и допълнителните изисквания, определени от компетентния надзорен орган.

е. Приложение 1 към Насоките за акредитация на сертификация предвижда предложените изисквания, които надзорният орган по защита на данните следва да включи и прилага по време на акредитацията на сертифициращ орган от националния орган по акредитация,

Комитетът счита, че:

2.2.1 ВЪВЕДЕНИЕ (Раздел 0 от проектните изисквания за акредитация на НО на Ирландия)

11. Комитетът приема факта, че условията за сътрудничество, регламентиращи взаимоотношенията между националния орган по акредитация и неговия надзорен орган по защита на данните, не са *сами по себе си* изискване за акредитация на сертифициращи органи. Но от съображения за пълнота и прозрачност Комитетът смята, че тези условия за сътрудничество, когато са налице, трябва да станат публични във формат, който НО счита за подходящ.

2.2.2 ТЕРМИНИ И ОПРЕДЕЛЕНИЯ

12. Комитетът отбелязва, че препратката към насоките за акредитация като „РД 261“ не е актуализирана. ЕКЗД прие Насоки 4/2018 относно акредитацията на сертифициращите органи съгласно член 43 от Общия регламент относно защитата на данните (2016/679). Поради това, Комитетът насърчава НО на Ирландия да измени формулировката и да препраща към Насоки 4/2018.

2.2.3 ОБЩИ БЕЛЕЖКИ

13. Комитетът отбелязва, че в проектните изисквания на НО на Ирландия многократно се упоменава „Компетентен надзорен орган“. Тъй като компетентният НО в този случай е самият НО на Ирландия, Комитетът препоръчва на НО на Ирландия да замени това споменаване с „Комисия за защита на данните“ или „НО на Ирландия“, за да се избегне объркване.

14. Комитетът приема, че проектните изисквания на НО на Ирландия включват раздел за термини и определения. Но някои от термините не се използват съгласувано в целия документ (напр. „предмет на оценка“ и „цел на оценка“). За да се избегне объркване, Комитетът препоръчва на НО на Ирландия да използва съгласувана терминология в проектните изисквания.

2.2.4 ОСНОВНИ ИЗИСКВАНИЯ ЗА АКРЕДИТАЦИЯ (Раздел 4 от проектните изисквания за акредитация)

15. По отношение на клауза 7 от подраздел 4.1.2 от проектните изисквания за акредитация на НО на Ирландия, Комитетът счита, че формулировката е не е достатъчно ясна по отношение на лицето, на което се предоставят основанията за одобряване на сертификацията. Освен това, не се разбира, какво се има предвид под „улесняване“ на регистъра. Поради тази причина, Комитетът препоръчва на НО на Ирландия да преработи проекта така, че да се внесе повече яснота.

2.2.5 ИЗИСКВАНИЯ ПО ОТНОШЕНИЕ НА СТРУКТУРАТА (Раздел 5 от проектните изисквания за акредитация)

16. Комитетът отбелязва, че в проектните изисквания за акредитация на НО на Ирландия се споменава за назначаването на „лице със съответния стаж, което да бъде отговорно за следенето на съответствието с изискванията на защита на данните и управлението на информацията“. Изискването за стаж трябва да бъде пояснено по отношение на опита и обхвата на правомощията на лицето. Освен това, функциите на това лице изглеждат сходни с тези на

длъжностно лице по защита на данните. Комитетът препоръчва на НО на Ирландия да разпише ясно функциите на това лице и да уточни съответния му опит.

2.2.6 ИЗИСКВАНИЯ ПО ОТНОШЕНИЕ НА РЕСУРСИТЕ (Раздел 6 от проектните изисквания за акредитация)

17. По отношение на персонала на сертифициращия орган (подраздел 6.1), Комитетът отбелязва, че изискванията за персонал с технически експертен опит, отговорен за вземане на решения, включват наличие на най-малко 5 години професионален опит, свързан с предмета на сертификацията, като персоналът, отговорен за оценките, трябва да притежава най-малко 2 години професионален опит. Също така, персоналът с юридически експертен опит, който взема решения, трябва да притежава най-малко 5 години професионален опит, а този, който отговаря за оценките, трябва да притежава най-малко 2 години. Комитетът отбелязва, че необходимият минимален професионален опит за служителите, отговарящи за вземането на решения, и тези, отговарящи за оценката, се различава значително. В тази връзка, Комитетът счита, че трябва да се обърне повече внимание на различните видове експертен опит, а не на годините професионален опит. Според Комитета оценителите трябва да притежават по-специализиран експертен и професионален опит в областта на техническите процедури (напр. одити и сертификации), а лицата, вземащи решения, трябва да притежават по-общ и всеобхватен експертен и професионален опит в областта на защитата на личните данни. В тази връзка Комитетът препоръчва на НО на Ирландия да обърне повече внимание на различните съществени познания и/или опит при оценителите и лицата, вземащи решения, като да намали разликата в необходимия професионален опит за тези длъжности.

2.2.7 ИЗИСКВАНИЯ КЪМ ПРОЦЕСИТЕ (Раздел 7 от проектните изисквания за акредитация)

18. По отношение на подраздел 7.10 от проектните изисквания за акредитация на НО на Ирландия („Промени, засягащи сертификацията“) Комитетът отбелязва, че процедурите за промени, които ще бъдат одобрявани съгласно раздел 7.10 от Приложението не са споменати. Комитетът препоръчва на НО на Ирландия да включи тази информация и да посочи някои от процедурите, които биха могли да бъдат въведени (напр. преходни периоди, процес на одобрение от компетентния НО и др.). Освен това, Комитетът счита, че промените в съвременните технологични науки също са релевантни и биха могли да повлияят на сертификацията. Поради тази причина Комитетът препоръчва на НО на Ирландия да включи тази възможност в списъка от промени, засягащи сертификацията. Накрая, Комитетът приветства включването на нарушенията на сигурността на личните данни и нарушенията на ОРЗД в списъка с промени, които биха могли да засегнат сертификацията. За да се гарантира яснота обаче, Комитетът препоръчва на НО на Ирландия да уточни, че нарушенията на сигурността на личните данни или нарушенията на ОРЗД трябва да се вземат под внимание само до степента, до която са свързани със сертификацията.

19. По отношение на промените, засягащи сертификацията (подраздел 7.10 от проектните изисквания на НО на Ирландия), и по-конкретно петото тире, Комитетът отбелязва, че НО на Ирландия се позовава на „приложими обвързващи решения на Европейския комитет по защита на данните“, както и на член 39 от Правилника на ЕКЗД, който „включва всички окончателни документи, приети от ЕКЗД“. За да се гарантира ясното разбиране на това, което се има предвид под „решения на Европейския комитет по защита на данните“, Комитетът препоръчва на НО на

Ирландия да поясни позоваването. Например, може да се включи препратка към „документи, приети от Европейския комитет по защита на данните“.

20. Комитетът отбелязва, че в подраздел 7.11 от проектните изисквания на НО на Ирландия (прекратяване, ограничаване, спиране на действието или оттегляне на сертификация) не се съдържа задължението, сертифициращият орган да приема решения и заповеди от НО на Ирландия за оттегляне или за отказ за издаване на сертификация на заявител, ако той вече не отговаря на изискванията за сертификация. Поради това, Комитетът препоръчва на НО на Ирландия да включи такова задължение.

3 ЗАКЛЮЧЕНИЯ/ПРЕПОРЪКИ

21. Проектните изисквания за акредитация на надзорния орган на Ирландия може да доведат до несъгласувано прилагане на акредитацията на сертифициращи органи, като е необходимо да се въведат следните промени:

22. По отношение на „Изискванията към процесите“ Комитетът препоръчва на НО на Ирландия:

1) да включи в подраздел 7.11 задължението, сертифициращият орган да приема решения и заповеди от НО на Ирландия за оттегляне или за отказ за издаване на сертификация на заявител, ако той вече не отговаря на изискванията за сертификация.

4 ЗАКЛЮЧИТЕЛНИ ЗАБЕЛЕЖКИ

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

24. Съгласно член 64, параграфи 7 и 8 от ОРЗД НО на Ирландия информира председателя по електронен път в срок от две седмици след получаване на становището дали ще измени или ще запази своя проект. В същия срок той предоставя изменения проект или, ако не възнамерява да се съобрази със становището на Комитета, той трябва да предостави съответните основания, поради които не възнамерява да се съобрази с това становище – изцяло или отчасти.

25. НО на Ирландия съобщава окончателното решение на Комитета, за да се включи в регистъра на решенията, които са били предмет на механизма за съгласуваност, в съответствие с член 70, параграф 1, буква ш) от ОРЗД.

За Европейския комитет по защита на данните

Председателят

(Andrea Jelinek)