Становище 4/2020 по проект за решение на компетентния надзорен орган на Обединеното кралство относно одобрението на изискванията за акредитация на сертифициращ орган съгласно член 43, параграф 3 (ОРЗД)

Прието на 29 януари 2020 г.

Прието

Съдържание

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 член 51, параграф 1, буква б) от Директива (ЕС) 2016/680 относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (наричана по-нататък „Директива за правоприлагане“),

като взе предвид Споразумението за Европейското икономическо пространство, 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 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. Целта на настоящото становище следователно 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 проектират своите изисквания за акредитация като спазват структурата, изложена в Приложението към Насоките 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 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 или регионални специфики и 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

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

влияние, например, върху доверието в независимостта или експертния опит на акредитираните сертифициращи органи.

(4) „Насоките 4/2018 относно акредитацията на сертифициращи органи съгласно член 43 от Общия регламент относно защитата на данните (2016/679)“ (по-нататък „Насоките“) и „Насоките 1/2018 относно сертифицирането и определянето на критерии за сертификация в съответствие с членове 42 и 43 от Регламент 2016/679“ ще служат като 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 само, изискванията, посочени в член 43, параграф 2. В сравнение със задълженията, свързани с акредитацията на сертифициращите органи от страна на националните органи по акредитация, в член 43 се дава по-малко информация относно изискванията за акредитация, когато самият надзорен орган извършва акредитацията. В интерес на осигуряването на хармонизиран подход към акредитацията, използваните от надзорния орган изисквания за акредитация следва да се ръководят от ISO/IEC 17065 и да се допълват от допълнителните изисквания, които надзорният орган определя в съответствие с член 43, параграф 1, буква б). ЕКЗД отбелязва, че в член 43, параграф 2, букви а)—д) са отразени и конкретизирани изискванията на ISO 17065, което допринася за съгласуваността. ([2])

(6) Становището на ЕКЗД се приема 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 решили, 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 Обединеното кралство внесе своите проектни изисквания за акредитация съгласно член 43, параграф 1, буква б) при ЕКЗД. Беше взето решение, с което се определя, че досието е пълно, и то беше оповестено на 25 октомври 2019 г. Националният орган по акредитация на Обединеното кралство ще извършва акредитация на сертифициращи органи, за да удостоверява използването на критерии за сертификация от ОРЗД. Това означава, че националният орган по акредитация ще използва ISO 17065 и допълнителните изисквания, определени от НО, след като бъдат одобрени от НО, в съответствие със становището на Комитета относно проектните изисквания, за да акредитира сертифициращи органи.

([2]) Параграф 39 от Насоките:

1. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf.

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 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 с 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 Обединеното кралство е решил да се обърне към своя национален орган по акредитация за издаване на акредитация, като е събрал допълнителните изисквания в съответствие с Насоките, които следва да се използват от националния орган по акредитация, когато издава сертификация.

4. Тази оценка на допълнителните изисквания за акредитация на НО на Обединеното кралство цели да проучи разликите (добавяния и заличавания) от Насоките и особено Приложението. 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 надзорните органи при определянето на изискванията им за акредитация. Приложението с насоки 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 надзорния орган.

6. Комитетът приема факта, че като се има предвид експертният 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 и последователно приложение и преглед според изискванията.

7. Комитетът отбелязва, че стандартите ISO, по-специално ISO 17065, са предмет на права на интелектуална собственост, поради което в 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 повтаря текста.

8. Накрая Комитетът извърши оценката си в съответствие със структурата, предвидена в Приложение 1 от Насоките. В случаите, когато настоящото становище не се изказва по конкретен раздел от проектните изисквания за акредитация на НО на Обединеното кралство, следва да се разтълкува, че Комитетът няма коментари и не иска от НО на Обединеното кралство да предприеме последващо действие.

9. В настоящото становище не се разглеждат въпроси, посочени от НО на Обединеното кралство, 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 от Насоките на ЕКЗД), заложени в изискванията за акредитация, с оглед извършване на преценка на следните положения:

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

б) независимост на сертифициращия орган;

в) конфликти на интереси на сертифициращия орган;

г) експертен опит на сертифициращия орган;

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

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

ж) 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 от 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 допълнителни проектни изисквания за акредитация)

11. Комитетът приема факта, че условията за сътрудничество, регулиращи 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.

12. Комитетът отбелязва факта, че НО на Обединеното кралство въвежда тези условия за сътрудничество с неговия националния орган по акредитация и че горепосочените условия ще бъдат достъпни на уебсайта на НО на Обединеното кралство, след като бъдат финализирани.

2.2.2 ОСНОВНИ ИЗИСКВАНИЯ ЗА АКРЕДИТАЦИЯ (Раздел 4 от допълнителни проектни изисквания за акредитация)

13. Във връзка с изискването за правна отговорност (подраздел 4.1.1) Комитетът отбелязва факта, че НО на Обединеното кралство изисква сертифициращият орган, който е акредитиран, *„да може да предостави доказателство за съответствие, както е заложено по време на процеса на акредитация“,* с ОРЗД и Закона за защита на данните на Обединеното кралство от 2018 г. За да се гарантира адекватна оценка и изпълнение на това изискване, Комитетът насърчава НО на Обединеното кралство да замени *„да може да предостави доказателство“* с „предоставя доказателство“. Поради това, Комитетът препоръчва на НО на Обединеното кралство да измени проекта по съответния начин.

14. Във връзка със споразумението за сертификация (подраздел 4.1.2), и по-специално изискване номер 8 (номер 9 в Приложението), Комитетът отбелязва факта, че НО на Обединеното кралство преформулира част от изискването, предвидено в Приложение 1 от Насоките. Въпреки това, НО на Обединеното кралство е пропуснал позоваване [където е приложимо] на „последствията за клиента също следва да се посочат“. Поради това, Комитетът препоръчва на НО на Обединеното кралство да допълни липсващата част от изискването, спомената по-горе.

15. Във връзка с употребата на печати и маркировки за защита на данните (подраздел 4.1.3), Комитетът отбелязва, че НО на Обединеното кралство изисква копие *„на печата/маркировката/логото да бъде предоставено на Информационния комисар за техните архиви“*. Като се има предвид, че маркировките и логата се използват не само от сертифициращия орган, но също и от собственика на схемата, Комитетът насърчава НО на Обединеното кралство да се позове също и на всички печати, маркировки и лога, предвидени във всяка схема за сертификация, одобрена от НО на Обединеното кралство.

2.2.3 ИЗИСКВАНИЯ ПО ОТНОШЕНИЕ НА РЕСУРСИТЕ (Раздел 6 от допълнителни проектни изисквания за акредитация)

16. Във връзка с персонала на сертифициращия орган (подраздел 6.1), и по- специално точка 6, Комитетът отбелязва факта, че НО на Обединеното кралство е предвидил, че: *„Персоналът, отговорен за решенията за сертификация, трябва да има значителен професионален*

експертен опит при определянето и прилагането на мерки за защита на данните“. Комитетът счита, че самият персонал, който взема решения за сертификация, може да няма „*значителен професионален опит при определянето и прилагането на мерки за защита на данните*“, но следва поне да има достъп до някого с такъв експертен опит, за да вземе информирано решение. Значителен професионален опит в прилагането на тези мерки, поне в ранните етапи, вероятно няма да бъде толкова широко разпространен в този сектор. Поради това, Комитетът насърчава НО на Обединеното кралство да изиска от сертифициращия орган да определи и обясни изискванията за професионален опит, които съответстват на схемата за сертификация.

2.2.4 ИЗИСКВАНИЯ КЪМ ПРОЦЕСИТЕ, член 43, параграф 2, буква в), г) (Раздел 7 от допълнителни проектни изисквания за акредитация)

17. Във връзка с главния подраздел относно изискванията за процесите (подраздел 7.1), и по-специално параграф 4, Комитетът отбелязва допълнителното изискване за органа по акредитация, за да се гарантира, че сертифициращият орган извършва разследване или одит в случаите, когато е поставено под въпрос съответствието с изискванията за защита на данните. Комитетът приема, че съответствието с изискванията за защита на данните се отнася до притежателя на сертификата. Това обаче следва ясно да се посочи в изискванията. Освен това Комитетът счита, че НО на Обединеното кралство трябва подробно да обясни, че тези разследвания следва да бъдат свързани с обхвата на сертифицирането и целта на оценката. Поради това, Комитетът препоръчва НО на Обединеното кралство да промени съответно своето изискване, като ясно определи, че спазването на защита на данните се отнася към притежателя на сертификата, и като посочи, че разследването следва да бъде свързано с обхвата на сертификация и целта на оценката.

18. Във връзка с приложението на изискванията за обработка (подраздел 7.2), Комитетът отбелязва нуждата сертифициращият орган да посочи „*дали се използват обработващи лични данни, а когато обработващите лични данни са заявители, техните отговорности и задачи трябва да бъдат описани, а заявлението трябва да съдържа съответните договори между администратора и обработващия лични данни“.* Като приема, че НО на Обединеното кралство е използвал формулировката на Приложение 1, Комитетът насърчава НО на Обединеното кралство да вземе предвид това дали отнасянето към съвместни администратори и техните специфични договорености трябва да бъде споменато в този случай.

19. Във връзка с методите за оценяване (подраздел 7.4), Комитетът отбелязва допълнителното изискване, предвидено от НО на Обединеното кралство, в което е заложено следното: „*В допълнение към точка 7.4.5 от ISO 17065, трябва да се предвиди, че съществуващата сертификация, която е свързана със същия предмет на сертификация, може да се вземе предвид като част от нова оценка […]“.* В тази връзка Комитетът счита, че е необходимо да се поясни допълнително, че в случаите, в които съществуващата сертификация е взета предвид като част от нова оценка, обхватът на горепосочената сертификация трябва също да бъде оценен подробно по отношение на съответствието със заложените критерии за сертификация. Поради това, Комитетът насърчава НО на Обединеното кралство да поясни формулировката.

20. Във връзка с изречението „*Може да се вземе предвид пълният доклад от оценка или информация, позволяваща оценка на предишната дейност по сертификация и резултатите*

от нея.“, Комитетът препоръчва на НО на Обединеното кралство да замени „може“ с „трябва“ в случаите, когато сертифициращият орган реши да вземе предвид съществуваща сертификация. В допълнение, Комитетът счита, че, за да бъде по-ясно, трябва да се назовава просто „сертификация“ вместо „дейност по сертификация“ и препоръчва на НО на Обединеното кралство да измени проекта. Освен това, позоваването на „предишна сертификация“ може да бъде подвеждащо, тъй като не се основава изрично на съществуващата сертификация, която сертифициращият орган иска да вземе предвид като част от своето собствено оценяване. Комитетът насърчава НО на Обединеното кралство да промени формулировката, за да поясни, че позоваването се отнася за съществуващата сертификация. Накрая Комитетът отбелязва, че сертифициращият орган следва да има достъп до доклада от оценката и всякаква друга информация, свързана с това, която позволява оценяването на дейността по сертификация, за да може да се вземе информирано решение. Поради тази причина, Комитетът насърчава НО на Обединеното кралство да поясни формулировката.

21. Освен това в параграфа, който започва с „*в допълнение към точка 7.4.6 от ISO 17065*“, Комитетът счита, че в случаите, когато надзорният орган на Обединеното кралство се позовава на „своя механизъм за сертифициране“, всъщност е имал предвид „схема за сертификация“. Поради това препоръчва на НО на Обединеното кралство да замени формулировката.

22. Във връзка с промените, засягащи сертификацията (подраздел 7.10), и по-специално четвъртия параграф („решения на Европейски комитет по защита на данните“), Комитетът приема, че НО на Обединеното кралство е използвал формулировката, предвидена в Приложение 1. За да се гарантира обаче ясното разбиране на това, което се има предвид с „решенията на Европейския комитет по защита на данните“, Комитетът насърчава НО на Обединеното кралство да поясни позоваването. Например, органа за защита на данните може да разясни, че става въпроси за „документи, приети от Европейския комитет по защита на данните“.

3 ЗАКЛЮЧЕНИЯ/ПРЕПОРЪКИ

23. Проектните изисквания за акредитация на надзорния орган на Обединеното кралство може да доведат до непоследователно приложение на акредитацията на сертифициращите органи и е необходимо да се направят следните промени:

24. Във връзка с „Основните изисквания за акредитация“ Комитетът препоръчва НО на Обединеното кралство:

    1. в подраздел 4.1.1 да замени изречението „следва да може да предостави доказателство“ с „може да предостави доказателство“;

    2. в подраздел 4.1.2 да включи липсващата част от изискването, така че да е в съответствие с текста от Приложение 1 на Насоките.

25. По отношение на „Изискванията към процесите“ Комитетът препоръчва на НО на Обединеното кралство:

    1. да измени подраздел 7.1, за да поясни, че спазването на защита на данните се отнася до притежателя на сертификата и че разследването следва да бъде свързано с обхвата на сертификация и целта на оценката;

2. да измени подраздел 7.4 като замени „може“ с „е“ и „сертифициращата дейност“ със „сертификация“;

3. да замени назоваването на „механизъм за сертифициране“ със „схема за сертификация“.

4 ЗАКЛЮЧИТЕЛНИ ЗАБЕЛЕЖКИ

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

27. Съгласно член 64, параграфи 7 и 8 от ОРЗД надзорният орган 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 спазва това становище, изцяло или отчасти.

За Европейския комитет по защита на данните

Председател

(Andrea Jelinek)