Становище 5/2020 по проект за решение на компетентния надзорен орган на Люксембург 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 се 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 определят 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 и регионални специфики и следва да вземат предвид

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

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) „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 Люксембург внесе своите проектни изисквания за акредитация съгласно член 43, параграф 1, буква а) в ЕКЗД. Беше взето решение, с което се определя, че досието е пълно, и то беше оповестено на 25 октомври 2019 г. НО на Люксембург ще извършва акредитация на сертифициращи органи, за да удостоверява използването на критерии за сертификация от ОРЗД.

([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 внесените проектни изисквания за акредитация

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 съгласно националното законодателство на НО на Люксембург е възложена задачата да извърши акредитацията на сертифициращите органи. За тази цел НО на Люксембург е разработил набор от изисквания специално за акредитацията на сертифициращи органи, съвместно с набор от критерии за сертификация, които трябва да бъдат официално одобрени.

Оценката на изискванията за акредитация цели да проучи вариациите (добавяния и заличавания) от Насоките, и особено Приложението. Освен това становището на ЕКЗД се фокусира върху всички аспекти, които могат да окажат влияние върху съгласувания подход, прилаган при акредитацията на сертифициращи органи.

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 НО.

Комитетът изпълни 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 Люксембург, следва да се разтълкува, че Комитетът няма коментари и не иска от НО на Люксембург да предприеме последващо действие. Комитетът отбелязва, че НО на Люксембург е предоставил информация, за да подпомогне оценяването на проектните изисквания за акредитация. Становището на Комитета посочва единствено проектните изисквания за акредитация.

Освен това в настоящото становище не се разглеждат въпроси, посочени от НО на Люксембург, 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 към 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.

3. 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 реши да провежда сам акредитацията на сертифициращите органи.

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

Комитетът счита, че:

2.2.1 ОБЩИ БЕЛЕЖКИ

4. Комитетът отбелязва, че проектните изисквания за акредитация не спазват напълно структурата, изложена в Приложение 1 към Насоките. Например липсват разделите „Приложно поле“ и „Термини и определения“. Във връзка с това, Комитетът отбелязва, че някои определения не се използват съгласувано в целия документ като например „клиент“ и „заявител“. За да се избегне объркване, използваните термини следва да бъдат приведени в съответствие с определенията в Насоките и Приложението, когато е възможно, и да се използват съгласувано. Следователно, с цел да се улесни оценяването, Комитетът насърчава НО на Люксембург да спазва структурата на Приложение 1 [към Насоките] по проектните изисквания за акредитация и да добави липсващите раздели.

5. Комитетът отбелязва, че в целия документ има няколко позовавания на изискванията „на този механизъм за сертифициране“ (например изискване 4.6.4) или на сертифициращите органи, които са акредитирани „съгласно (...) механизъм за сертифициране“ (например изискване 2.2.2). Позоваването на механизма за сертифициране изглежда, че е въпрос на изготвяне на проекта. Поради тази причина, Комитетът насърчава НО на Люксембург да преработи позоваванията, за да отрази, че сертифициращите органи са акредитирани съгласно изискванията, одобрени от надзорния орган.

6. Аналогично позоваването на „изискванията, изложени в този механизъм за сертифициране“, използвано в целия документ (например изискване 1.1.1.2), е объркващо. По-подходяща формулировка може да бъде „критерии, изложени в механизма за сертифициране“. По този начин Комитетът насърчава НО на Люксембург да поясни позоваванията на „механизъм за сертифициране“ в целия документ.

7. Комитетът отбелязва, че няколко изисквания (например 3.2.1.1 и 4.1.2) се отнасят до „съответните международни стандарти, „съответния стандарт“ или „определения стандарт“. Въпреки това определение за тези стандарти не е дадено и следователно не е ясно кои са цитираните стандарти. Поради това, Комитетът препоръчва на НО на Люксембург да поясни значението на тези стандарти. Това може да се направи например в разделите „Приложно поле“ или „Термини и определения“.

2.2.2 ОСНОВНИ ИЗИСКВАНИЯ ЗА АКРЕДИТАЦИЯ

8. Комитетът отбелязва, че изискване 1.1.1.1 на НО на Люксембург се позовава на друг стандарт („ISAE 3000“), който ЕКЗД не е оценил. Поради това, Комитетът препоръчва на НО на Люксембург да поясни, че изискванията не могат да бъдат обезсилени от външен стандарт, например от ISAE 3000.

9. Комитетът отбелязва, че изискванията в 1.6 не включват задължението на сертифициращия орган да публикува и да улесни обществения достъп до всички версии на одобрените критерии и всички процедури за сертифициране, определени в Приложението към Насоките (раздел 4.6). Комитетът отбелязва, че НО на Люксембург може да бъде собственик на схема за сертификация, но Комитетът счита, че ще е от помощ да се добави подходяща препратка, за да се гарантира, че критериите са актуални и лесно достъпни чрез самия сертифициращ орган. В тази връзка Комитетът счита, че ако направи информацията достъпна единствено при поискване, както е изложено в изискване 1.6.1, НО на Люксембург определя по-стриктно изискване от Приложението, в което е заложено, че информацията трябва да бъде леснодостъпна за обществеността. Поради това, Комитетът препоръчва на НО на Люксембург да измени изискването, за да включи задължението на сертифициращия орган да осигури лесен обществен достъп до всички версии на одобрените критерии и всички процедури по сертифициране в съответствие с Приложението към Насоките.

10. Комитетът отбелязва, че изискване 1.2.4 се отнася до „сертифицирана обработка“. Комитетът счита, че може да се използва по-прецизна формулировка в съответствие с Насоките, например „операции/дейности по сертифицирана обработка“. Това предоставя по-широк обхват на сертификацията, както е предвидено от ОРЗД. Поради това, Комитетът насърчава НО на Люксембург съответно да измени проектните изисквания.

2.2.3 ИЗИСКВАНИЯ ПО ОТНОШЕНИЕ НА РЕСУРСИТЕ

11. Комитетът отбелязва, че изискване 3.1.1.2 изглежда повтарящо се и неясно, като различната терминология не е помогнала. Например, третият параграф се тълкува сякаш ангажираният партньор самостоятелно взема решението за пригодността на тяхното решение. Комитетът препоръчва на НО на Люксембург да направи изискването по-ясно и по-разбираемо и да използва съгласувана терминология.

2.2.4 ИЗИСКВАНИЯ КЪМ ПРОЦЕСИТЕ

12. Комитетът отбелязва, че изискване 4.2.1 представя няколко примера за необходима информация. Въпреки това първите два представени примера могат да бъдат включени като самостоятелни изисквания в съответствие с раздел 7.2 от Приложение 1 към Насоките. Поради това, Комитетът насърчава НО на Люксембург да измени формулировката и да включи гореспоменатите примери като изисквания.

13. Във връзка с раздел 4.4 („Оценка“) от изискванията за акредитация на НО на Люксембург, Комитетът е на мнение, че изискванията за акредитация следва да включват задължение за сертифициращия орган да гарантира, че има въведени методи за оценяване и че тези методи за оценяване, описани в механизма за сертифициране, са стандартизирани и общоприложими. Това ще гарантира, че се използват сравними методи за преценка за съпоставими области на оценяване. Всяко отклонение от тези методи за преценка е нужно да бъде обосновано от сертифициращия орган. Поради това, Комитетът препоръчва на НО на Люксембург да измени проекта, за да включи гореспоменатото задължение на сертифициращия орган.

14. Освен това Комитетът отбелязва, че в изискване 4.4.2 се посочва, че въпреки, че прехвърлянето на дейността на трети лица не е позволено, сертифициращият орган да може да използва външни експерти за конкретни области. В тази връзка е важно да се поясни, че сертифициращият орган ще запази отговорността за вземане на решения, дори когато използва външни експерти. Поради тази причина, Комитетът препоръчва на НО на Люксембург съответно да измени формулировката в изискване 4.4.2.

15. Комитетът отбелязва, че раздел 4.7 от изискванията за акредитация на надзорния орган на Люксембург („Документация по сертифициране“) не посочва изискването в Приложението за документиране на периода за наблюдение (раздел 7.9). Поради това, Комитетът насърчава НО на Люксембург да включи период за контрол по смисъла на раздел 7.9 относно наблюдението.

16. Във връзка с раздел 4.8 („ Указател на дейности по сертифицирана обработка“) от изискванията за акредитация на НО на Люксембург, в изискване 4.8.1 се посочва, че информацията ще стане обществено достояние „при поискване“. Комитетът е на мнение, че задължението за прозрачност, изложено в раздел 7.8 от Приложение 1, ще се изпълни по-добре, ако се даде достъп до информацията по инициатива на сертифициращия орган. По този начин, Комитетът препоръчва на НО на Люксембург да измени проекта, за да гарантира, че сертифициращият орган ще даде обществен достъп до информацията, посочена в раздел 7.8 от Приложение 1 към Насоките.

17. Комитетът отбелязва, че раздел 4.8 разглежда извършването на наблюдение, без никакви изисквания. Комитетът препоръчва на НО на Люксембург да изясни начина, по който ще се извърши мониторингът.

18. Във връзка с прекратяването, намаляването, преустановяването или оттеглянето на сертификация (подраздел 4.10), Комитетът отбелязва, че не се посочва задължението на сертифициращия орган да приема решения и нареждания от компетентния надзорен орган да оттегли или да не издава сертификат на клиент (заявител), ако не са спазени или вече не са спазени изискванията за сертификация. Това задължение е изложено в член 58, параграф 2, буква з) от ОРЗД, както и в раздел 7.11 от Приложение 1. Следователно, Комитетът препоръчва на НО на Люксембург да измени изискванията за акредитация, посочващи правилата, обхващащи оттеглянето, прекратяването, намаляването или преустановяването на сертификацията.

19. Комитетът отбелязва, че раздел 9 от Приложението, свързан с общия преглед, не съдържа изисквания. Например, тук не е обхванат раздел 9.3.4 относно преустановяването или оттеглянето на акредитация. Това са важни въпроси, които гарантират препратки към съответните раздели или изисквания, които са добавени. Комитетът насърчава НО на Люксембург да поясни къде са обхванати изискванията.

3 ЗАКЛЮЧЕНИЯ/ПРЕПОРЪКИ

20. Проектните изисквания за акредитация на надзорния орган на Люксембург може да доведат до несъгласувано прилагане на акредитацията на сертифициращи органи и е необходимо да се направят следните промени:

21. Основно Комитетът препоръчва на надзорния орган на Люксембург:

    1. да поясни значението на думата „стандарт“, както е използвана в няколко изисквания (например 3.2.1.1 и 4.1.2). Това може да се направи например в разделите „Приложно поле“ или „Термини и определения“.

22. Във връзка с „Основните изисквания за акредитация“ Комитетът препоръчва на НО на Люксембург:

    1. да поясни, че изискванията не могат да бъдат обезсилени от външен стандарт, например ISAE 3000;

    2. да измени изискванията в 1.6, за да включи задължението на сертифициращия орган да публикува и да осигури лесен обществен достъп до всички версии на одобрените критерии и всички процедури по сертифициране в съответствие с Приложението към Насоките.

23. По отношение на „Изисквания относно ресурсите“ Комитетът препоръчва на НО на Люксембург:

    1. да преработи изискване 3.1.1.2, за да го направи по-ясно и по-разбираемо, като използва съгласувана терминология.

24. По отношение на „Изискванията към процесите“ Комитетът препоръчва на НО на Люксембург:

    1. да измени раздел 4.4 от проектните изисквания, за да включи задължението на сертифициращия орган да гарантира, че са въведени методи за оценяване и че тези методи за оценяване, описани в механизма за сертифициране, са стандартизирани и

общоприложими. Всяко отклонение от методите на оценяване е нужно да бъде обосновано от сертифициращия орган.

2. да измени формулировката в изискване 4.4.2, за да се посочи изрично, че сертифициращият орган ще запази отговорността за вземане на решения, дори когато използва външни експерти;

3. да измени раздел 4.8 от своите проектни изисквания за акредитация, за да гарантира, че сертифициращият орган ще даде обществен достъп до информацията, посочена в раздел 7.8 от Приложение 1 от Насоките;

4. да поясни в раздел 4.8 начина, по който ще се извърши мониторингът;

5. да измени подраздел 4.10, за да посочи правилата, обхващащи оттеглянето, прекратяването, намаляването или преустановяването на сертификацията.

4 ЗАКЛЮЧИТЕЛНИ ЗАБЕЛЕЖКИ

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

26. 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)