Становище 15/2020 по проект на решение на компетентните надзорни органи на Германия относно одобрението на изискванията за акредитация на сертифициращ орган съгласно член 43, параграф 3 (ОРЗД)

Прието на 25 май 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 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 постига 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 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 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 сертифициращите 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 критериите за сертифициране в

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

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 КРАТКО ИЗЛОЖЕНИЕ НА ФАКТИТЕ

1. Германските надзорни органи на Федерацията и на провинциите (по-нататък „НО на Германия“) внесоха своите проектни изисквания за акредитация съгласно член 43, параграф 1, буква б) при ЕКЗД. Досието беше счетено за пълно на 13 февруари 2020 г. Националният орган по акредитация (НОА) на Германия, DAkkS, ще извършва акредитация на сертифициращи органи, за да удостоверява използването на критерии за сертифициране от ОРЗД. Това означава, че НОА ще прилага ISO 17065 и допълнителните изисквания, определени от НО на Германия, след като бъдат одобрени от същия орган, в съответствие със становището на Комитета относно проекта на 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 сертифициращи органи съгласно член 43 от Общия регламент относно защитата на данните, параграф 39. Достъпни на: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_bg.pdf

2 ОЦЕНКА

2.1 Обща обосновка на ЕКЗД относно внесения проект на решение

3. Целта на настоящото становище е да оцени изискванията за акредитация, разработени от НО, или 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 Германия са решили да прибягнат към съвместна акредитация от национален орган по акредитация (НОА), DAkkS, и компетентния НО, за издаване на акредитация, като са изпълнили допълнителните изисквания в съответствие с Насоките, които следва да се прилагат, когато издават акредитация.

4. Тази оценка на допълнителните изисквания за акредитация на НО на Германия цели да проучи разликите (добавяния и заличавания) от Насоките, особено приложение 1 към 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 надзорните органи 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 експертният им опит, на НОА и компетентните НО, когато е приложимо, следва да бъде дадена свобода за действие, когато определят конкретни специфични разпоредби в рамките на приложимите изисквания за акредитация. Комитетът обаче 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 към Насоките (по-нататък „приложение“). В случаите, когато в настоящото становище няма тълкуване на конкретен раздел от проекта на акредитационни изисквания на НО на Германия, следва да се счита, че Комитетът няма коментари и не препоръчва на НО на Германия да предприемат последващо действие.

9. В настоящото становище не се разглеждат въпроси, посочени от НО на Германия, 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 предоставят, 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 сертифициране 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 от Насоките за акредитация на сертификация предвижда предложените изисквания, да бъдат изготвени и прилагани от надзорният орган по защита на данните по време на акредитацията на сертифициращ орган от националния орган по акредитация;

Комитетът счита, че:

2.2.1 УВОД

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. От съображения за пълнота и прозрачност, обаче, 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 в глава 3 („Определения“) от проекта на акредитационни изисквания на НО на Германия са определени типовете допустими схеми за сертифициране, като е посочено, че те трябва да отговарят на изискванията по EN ISO/IEC 17065 на Немския институт за стандартизация. В тази връзка следва да се отбележи, че в раздели 5.1 и 5.2 от Насоките на ЕКЗД вече е определено по изчерпателен начин какво може да бъде сертифицирано по ОРЗД. Следователно, Комитетът признава, че намерението на НО на Германия не е да ограничат заявеното в Насоките и че твърденията в глава 3 от проекта на акредитационни изисквания на НО на Германия трябва да се считат за приложими по отношение на тези изисквания за акредитация.

2.2.3 ОБЩИ БЕЛЕЖКИ

13. Комитетът отбелязва, че разделът с „общи бележки“ в проекта на акредитационни изисквания на НО на Германия се отнася до „разрешаването“ на критериите за сертифициране от ЕКЗД „в съответствие с член 63 и член 64, параграф 1, буква в) от ОРЗД“. Комитетът отбелязва, че ОРЗД не предоставя на ЕКЗД компетентността да „разрешава“ критерии за сертифициране. Според горепосочените членове обаче ЕКЗД може да одобрява критерии за сертифициране. Следователно, Комитетът препоръчва на НО на Германия да заличат позоваването на „разрешаване от ЕКЗД“, за да приведат проекта в съответствие с формулировката на ОРЗД.

2.2.4 ОСНОВНИ ИЗИСКВАНИЯ ЗА АКРЕДИТАЦИЯ (глава 4 от проекта на акредитационни изисквания)

14. Що се отнася до изискването за правна отговорност (раздел 4.1 от проекта на акредитационни изисквания на НО на Германия), Комитетът отбелязва, че в съпътстващия документ, НО на Германия обясняват, че от сертифициращия орган се очаква да разполага с актуални процедури и следователно не е необходимо да се добавят допълнителни изисквания.. Комитетът обаче счита, че очакваното не задължава сертифициращите органи да разполагат с такива процедури. Както е предвидено в раздел 4.1.1 от Приложението към Насоките, сертифициращите органи разполагат с актуални процедури, които доказват спазване на правните отговорности, изложени в условията за акредитация. Освен това, сертифициращият орган е в състояние да представи доказателство за отговарящи на ОРЗД процедури и мерки, по-специално, за контролиране и разглеждане на личните данни на клиентската организация като част от процеса по сертифициране. Следователно, Комитетът препоръчва на НО на Германия да изменят проекта на изисквания, за да го приведат в съответствие с Насоките.

15. Що се отнася до подраздел 4.1.2.2 от проекта на акредитационни изисквания на НО на Германия („споразумение за сертифициране“), Комитетът отбелязва, че проектът на изисквания за сертифициране на НО на Германия не включва задължението да се осигури пълна прозрачност на компетентния НО във връзка с процедурата за сертифициране, включително, поверителни въпроси от договорно естество. Освен това не се споменава задължението на заявителя да предостави на сертифициращия орган достъп до неговите дейности по обработване. Поради това, Комитетът препоръчва на НО на Германия да включат горепосочените задължения в своя проект.

16. Комитетът отбелязва, че изричното позоваване на задачите и правомощията на компетентния НО (раздел 4.1.2, трето тире от Приложението) не е включено в подраздел 4.1.2.2 от проекта на акредитационни изисквания на НО на Германия. Комитетът счита, че това позоваване следва да се добави в проекта на изисквания и следователно препоръчва на НО на Германия да изменят документа по съответния начин.

17. Освен това, проектът на изисквания на НО на Германия относно споразумението за сертифициране не включва задължението да се даде възможност на сертифициращия орган да оповестява цялата необходима информация за издаване на сертификат съгласно член 42, параграф 8 и член 43, параграф 5 от ОРЗД (раздел 4.1.2, седмо тире от Приложението). Въпреки че това задължение е включено в раздела относно управление на процесите от проекта на акредитационни изисквания на НО на Германия, Комитетът счита, че то следва да бъде част от споразумението за сертифициране, за да се укрепи неговият обвързващ характер. Поради това Комитетът препоръчва на НО на Германия да включат горепосоченото задължение като част от елементите от споразумението за сертифициране.

18. Според Приложението заявителят трябва да уведомява сертифициращия орган за значителни промени в своето фактическо или правно положение, <u>както и в своите продукти, процеси и услуги, които касаят сертифицирането</u> (раздел 4.1.2, десето тире от Приложението). В проекта на акредитационни изисквания на НО на Германия обаче раздел 4.1.2.2, шесто тире е включено единствено задължението за уведомяване на сертифициращия орган за значителни промени в действителните или правните обстоятелства, но не се споменават изрично продуктите, процесите и услугите. Комитетът препоръчва на НО на Германия да включат такова позоваване в съответствие с Приложението.

19. Що се отнася до подраздел 4.2.7 от проекта на акредитационни изисквания на НО на Германия („безпристрастно разглеждане“), Комитетът препоръчва да се завишат критериите, приложими към сертифициращите органи, които принадлежат към отделен правен субект или са под негов контрол, за да се вземе под внимание фактът, че всеки вид икономически отношения между сертифициращия орган и правния субект, в зависимост от своите характеристики, може да се отрази на безпристрастността на неговите дейности по сертифициране.

20. Що се отнася до раздел 4.6 от проекта на акредитационни изисквания на НО на Германия („публично достъпна информация“), Комитетът отбелязва, че не се споменава публикуването на <u>всички версии</u> на одобрените критерии и на <u>процедурите по сертифициране.</u> Следователно, Комитетът насърчава НО на Германия да изменят проекта на акредитационни изисквания, за да подчертаят изрично, че публикуването включва всички версии на одобрените критерии и процедурите по сертифициране. Освен това, Комитетът отбелязва, че раздел 4.6, втори параграф гласи, че „ в повечето случаи *трябва да се публикуват* схемите за сертифициране, използвани от сертифициращия орган, одобрените критерии в съответствие с член 42,

параграф 5 от ОРЗД, в които е заложен разрешения срок на прилагането.“ За да се избегне неяснотата, Комитетът насърчава германските надзорни органи да заличат думата „в повечето случаи“ и да включат „и“ между „сертифициращ орган“ и „одобрените критерии“.

2.2.5 ИЗИСКВАНИЯ ПО ОТНОШЕНИЕ НА РЕСУРСИТЕ (глава 6 от проекта на акредитационни изисквания)

21. Що се отнася до изискванията за експертни знания, и по-специално, подраздел 6.1.2.1 от проекта на изисквания за акредитация на НО на Германия („компетентност на човешките ресурси“), Комитетът отбелязва, че в изискванията относно знания в изброените области не се споменава, че знанията трябва да са уместни и подходящи. За да се гарантира съгласуваност с нивото на експертни знания, изисквано в Приложението, Комитетът препоръчва на НО на Германия да приведат формулировката в съответствие с Насоките, като изискат знанията да са уместни и подходящи.

22. Освен това Комитетът отбелязва, че изискванията за персонал с технически опит, отговорен за вземането на решения, включват най-малко 7 години професионален опит или 5 години професионален опит по техническа защита на данните в зависимост от образователното равнище, докато персоналът, отговорен за оценките, следва да има 4 години професионален опит или 2 години професионален опит по техническа защита на данните и опит в процедурата, която се прилага при тестване в зависимост от образователното равнище. Също така, персоналът с юридически експертен опит, който взема решения, трябва да притежава най-малко 5 години професионален опит по право в областта на защитата на данните, а този, който отговаря за оценките, трябва да притежава най-малко 2 години опит по право в областта на защитата на данните и на одитните процедури. 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 изискванията за компетентност за оценителите и вземащите решения лица следва да бъдат пригодени, така, че да се вземат под внимание различните задачи, които те изпълняват, вместо броят на годините натрупан опит. Комитетът счита, че 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 изчерпателен експертен и професионален опит в областта на защитата на личните данни. Поради тази причина Комитетът препоръчва на НО на Германия да обърнат повече внимание на различните съществени познания и/или опит при оценителите и лицата, вземащи решения, както и да намалят разликата в необходимия професионален опит за тези длъжности.

23. Освен това Комитетът счита, че познаването на системите за управление, свързани с областта на сертифициране, следва да бъде разширено до ISO/IEC 27701:2019 — Методи за сигурност.– Допълнение към ISO/IEC 27001 и ISO/IEC 27002 за управление на неприкосновеността на информацията — Изисквания и указания, и насърчава НО на Германия да включат такова позоваване.

24. И накрая, що се отнася до изискванията за образование на техническия персонал, Комитетът счита, че списъкът с предмети вече е пригоден към техническия опит, изискван в Приложението. Следователно, Комитетът насърчава НО на Германия да заличат позоваването на „природни науки“ от списъка с предмети във връзка с висшето образование на техническия персонал.

2.2.6 ИЗИСКВАНИЯ КЪМ ПРОЦЕСИТЕ (глава 7 от проекта на акредитационни изисквания)

25. Комитетът отбелязва, че в глава 7 от проекта на изисквания за акредитация на НО на Германия на няколко пъти се споменава изразът „неговите критерии“ (напр. в раздели 7.4, 7.6, 7.11 и 7.13). За да се избегне неяснотата, Комитетът насърчава НО на Германия да пояснят значението на този израз, като например добавят обяснение в Допълнение 1 (Речник).

26. Що се отнася до раздел 7.1 от проекта на изисквания за акредитация на НО на Германия („обща информация“), Комитетът отбелязва, че няма изрично позоваване на задължението на сертифициращия орган да спазва допълнителните изисквания. Въпреки че такова задължение би могло да се подразбира от текста на проектните изисквания, Комитетът счита, че следва да се включи изрично позоваване на горепосоченото задължение. Поради това, Комитетът препоръчва на НО на Германия да изменят проекта.

27. Комитетът отбелязва, че в допълнителните проектни изисквания на НО на Германия не се споменава употребата на одобрения Европейски печат за защита на данните съгласно раздел 7.1.2 от Приложението. Комитетът счита, че следва да се включи такова споменаване, особено като се има предвид, че акредитацията на сертифициращ орган, който предоставя европейски печати за защита на данните, може да трябва да се извърши във всяка от държавите членки, в които е установен сертифициращият орган.[3] Поради това, Комитетът препоръчва на НО на Германия да включат горепосоченото споменаване. Например, проектните изисквания биха могли да гласят следното: *„Компетентният НО се уведомява, преди сертифициращ орган да започне да използва одобрен европейски печат за защита на данните в нова държава членка от сателитен офис“.*

28. Комитетът отбелязва, че в раздел 7.2 („заявление“) от проекта на акредитационни изисквания на НО на Германия е предвидена ситуацията, в която се използват обработващи лични данни за извършване на операции по обработване на данни в съответствие с Приложението към Насоките. Комитетът отбелязва обаче, че когато се използват обработващи лични данни, заявлението съдържа договора(ите) на съответния администратор/обработващ лични данни, както е посочено в Приложението. Следователно, Комитетът препоръчва на НО на Германия да приведат формулировката в съответствие с Насоките, като включат споменаването на договора(ите) на администратора/обработващия лични данни. Освен това Комитетът насърчава НО на Германия да обмислят, дали в този случай следва да се направи също споменаване на съвместни администратори и специфичните условия за тях.

29. Комитетът отбелязва, че в раздел 7.2 от проекта на акредитационни изисквания на НО на Германия е посочено, че „администраторът на лични данни и обработващият лични данни имат право да подадат заявление за сертифициране“. Възможността на обработващия лични данни да подаде заявление за сертифициране ще зависи от специфичната схема за сертифициране. Следователно, за да се избегне объркване, Комитетът насърчава НО на Германия да заличат позоваването по-горе или да пояснят, че възможността обработващите лични данни да бъдат сертифицирани ще зависи от обхвата на схемата за сертифициране.

30. Що се отнася до раздел 7.3 от проекта на акредитационни изисквания на НО на Германия („заявления за оценка“), Комитетът отбелязва, че тези изисквания гласят, че „планираните

[3] В тази връзка вж. Насоки 1/2018, параграф 44.

методи на оценка са предвидени в договора [...]“. За да се поясни, че това е изискване, Комитетът насърчава НО на Германия да преработят първия параграф, за да изяснят, че методите на оценка трябва да бъдат включени в споразумението за сертифициране, т.е. да преработят изискването, така че то да гласи „планираните методи на оценка трябва да бъдат предвидени в договора [...]“. Освен това, Комитетът насърчава НО на Германия да заменят позоваването в раздел 7.3.1.б на ISO 17065 с раздел 7.3 от ISO 17065, за да го приведат в съответствие с формулировката на Приложението. Също така Комитетът отбелязва, че четвъртият параграф се отнася до подходящите технически и правни компетентности. За по-голяма яснота, Комитетът насърчава НО на Германия да добавят „в сферата на защитата на данните“.

31. Комитетът отбелязва, че раздел 7.4 от проекта на акредитационни изисквания на НО на Германия („методи на оценка“) не включва задължението на сертифициращия орган да описва достатъчно методи на оценка за извършване на преценка на съответствието на операцията(ите) по обработване с критериите за сертифициране. Комитетът препоръчва на НО на Германия да изменят проектните изисквания, за да включат тази информация. Пример за това би бил да се добави следното: *„Сертифициращият орган гарантира, че механизмите, използвани за издаване на сертификат, описват достатъчни методи на оценка за извършване на преценка на съответствието на операцията(ите) по обработване с критериите за сертифициране“.* Освен това, що се отнася до първата област, която ще бъде обхванатата от методите на оценка, Комитетът счита, че нейната необходимост и пропорционалност се оценява, ако е приложимо, също и по отношение на съответните субекти на данни.. И накрая, Комитетът отбелязва, че не се споменава документирането на методи и констатации. Поради това, Комитетът насърчава НО на Германия да изменят проектните изисквания и изрично да включат тази информация.

32. Що се отнася до съществуващите сертификати (раздел7.4 от проекта на акредитационни изисквания на НО на Германия), Комитетът счита, че четвърто тире на страница 13 е подвеждащо, тъй като не е ясна връзката между периодите на валидност на текущия и предходния сертификат и по какъв начин те биха се съчетали. Освен това не изглежда възможно да се оспори валидността на издаден по-рано сертификат от различен акредитиран сертифициращ орган. В обобщение би било от полза да се внесе яснота в параграфа относно връзката между споменатите различни елементи. Комитетът препоръчва на НО на Германия да изменят проекта, по-специално, като пояснят, че срокът на валидност на сертифицирането по ОРЗД не трябва да зависи от валидността на други типове сертификати.

33. Що се отнася до раздел 7.5 („оценяване“) от проекта на акредитационни изисквания на НО на Германия, Комитетът насърчава НО на Германия да променят заглавието на раздела на „преглед“.

34. Що се отнася до промените, които засягат сертифицирането (раздел 7.10 от проекта на акредитационни изисквания на НО на Германия), Комитетът отбелязва, че в изискванията е посочено, че „клиентът се уведомява своевременно за промените в правната рамка, които се отнасят до него“. Като се има предвид необходимостта от запазване на безпристрастността на сертифициращия орган, Комитетът насърчава НО на Германия да преформулират изречението, за да пояснят, че на клиента своевременно се предоставя обща информация относно промените, които може да го засягат. Освен това, за да се гарантира ясното разбиране на това, което се има предвид под „решенията на Европейския комитет по защита на данните“, Комитетът насърчава НО на Германия да пояснят позоваването. Даден пример може да бъде „документи, приети от Европейския комитет по защита на данните“.

35. Комитетът отбелязва, че в подраздел 7.11 от проекта на изисквания на НО на Германия (прекратяване, ограничаване, спиране на действието или оттегляне на сертификация) не се съдържа задължението сертифициращият орган да приема решения и заповеди от НО на Германия 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 Германия да включи такова задължение. Освен това Комитетът насърчава НО на Германия да заменят думата „ограничаване“ с „намаляване“ в заглавието на раздела в съответствие с приложението към Насоките.

2.2.7 ОЩЕ ДОПЪЛНИТЕЛНИ ИЗИСКВАНИЯ

36. Що се отнася до подраздел 8.11.3 от акредитационните изисквания на НО на Германия („разглеждане на жалби“), Комитетът насърчава германските надзорни органи да заменят позоваването на „основателни жалби“ с „обосновани жалби“, за да се осигури повече яснота.

3 ЗАКЛЮЧЕНИЯ/ПРЕПОРЪКИ

37. Проектът на акредитационни изисквания на германските надзорни органи на Федерацията и провинциите може да доведе до несъгласувано прилагане на акредитацията на сертифициращи органи, затова е необходимо да се въведат следните промени:

38. Що се отнася до общите забележки, Комитетът препоръчва на НО на Германия:

    1) да заличат позоваването на „разрешаване от ЕКЗД“, за да приведат проекта в съответствие с формулировката на ОРЗД.

39. Що се отнася до основните изисквания за акредитация, Комитетът препоръчва НО на Германия:

    1) да изменят изискванията относно правната отговорност (подраздел 4.1), за да ги приведат в съответствие с Насоките.

    2) да изменят подраздел 4.1.2.2, за да включат в споразумението за сертифициране задължението да се осигурява пълна прозрачност на НО на Германия във връзка с процедурата по сертифициране и да се предостави на сертифициращия орган достъп до дейностите по обработване на заявителя.

    3) да включат в подраздел 4.1.2.2 изрично позоваване на задачите и правомощията на компетентния НО в съответствие с Приложението.

    4) да включат в елементите на споразумението за сертифициране задължението да се даде възможност на сертифициращия орган да оповестява цялата необходима информация за издаване на сертификат съгласно член 42, параграф 8 и член 43, параграф 5 от ОРЗД.

    5) да включат изрично позоваване на „продуктите, процесите и услугите, обхванати от сертифицирането“ в шесто тире от подраздел 4.1.2.2.

    6) да се укрепят в раздел 4.2.7 критериите, приложими към сертифициращите органи, които принадлежат към отделен правен субект или са под негов контрол,

за да се вземе под внимание фактът, че всеки вид икономически отношения между сертифициращия орган и правния субект, в зависимост от своите характеристики, може да се отрази на безпристрастността на неговите дейности по сертифициране.

40. Що се отнася до изискванията относно ресурсите, Комитетът препоръчва на НО на Германия:

1) да приведат формулировката на подраздел 6.1.2.1 в съответствие с насоките, като изискат знанията да са уместни и подходящи.

41. Що се отнася до изискванията към процесите, Комитетът препоръчва на НО на Германия:

1) да изменят раздел 7.1., за да се включи изрично позоваване на задължението на сертифициращия орган да спазва допълнителните изисквания.

2) да включат позоваване на използването на одобрен европейски печат за защита на данните.

3) да приведат формулировката на раздел 7.2 в съответствие с Насоките, като включат позоваване на договора(ите) на администратора/обработващия лични данни.

4) да включат в раздел 7.4 задължението на сертифициращия орган да опише достатъчно методи за оценка на съответствието на операцията(ите) по обработване с критериите за сертифициране.

5) да поясняват в раздел 7.4, че срокът на валидност на сертифицирането по ОРЗД не трябва да зависи от валидността на други типове сертификати.

6) да включат в подраздел 7.11 задължението сертифициращият орган да приема решения и заповеди от НО на Германия за оттегляне или за отказ за издаване на сертификация на заявител, ако изискванията за сертификация вече не се спазват.

4 ЗАКЛЮЧИТЕЛНИ ЗАБЕЛЕЖКИ

42. Настоящото становище е адресирано до германските надзорни органи на Федерацията и провинциите и ще бъде оповестено публично съгласно член 64, параграф 5, буква б) от ОРЗД.

43. Съгласно член 64, параграфи 7 и 8 от ОРЗД НО на Германия трябва да информират председателя по електронен път в срок от две седмици след получаване на становището дали ще изменят или ще запазят своето проекторешение. В същия срок те следва да предоставят изменения проект на решение или, ако не възнамеряват да се съобразят със становището на Комитета, те трябва да предоставят съответните основания, поради които не възнамеряват да го направят — изцяло или отчасти.

44. НО на Германия съобщават 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

Председател

(Андреа Йелинек)