Насоки 4/2018 относно акредитацията на сертифициращи органи съгласно член 43 от Общия регламент относно защитата на данните (2016/679)

Версия 3.0

4 юни 2019 г.

Прието

История на версиите

Версия 3.0	4 юни 2019 г.	Включване на приложение 1 (версия 2.0 на приложение 1, приета на 4 юни 2019 г. след обществена консултация)
Версия 2.0	4 декември 2018 г.	Приемане на насоките след обществена консултация — на същата дата приложение 1 (версия 1.0) беше прието за обществена консултация
Версия 1.0	6 февруари 2018 г.	Приемане на Насоките от работната група по член 29 (версия за обществена консултация). Тази версия е одобрена от ЕКЗД на 25 май 2018 г.

Съдържание

Европейският комитет по защита на данните,

като взе предвид член 70, параграф 1, буква д) 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 и

след като разгледа резултатите от обществените консултации относно насоките, проведени през февруари 2018 г., и относно приложението, проведени между 14 декември 2018 г. и 1 февруари 2019 г., в съответствие с член 70, параграф 4 от ОРЗД,

ПРИЕ СЛЕДНИТЕ НАСОКИ:

1 ВЪВЕДЕНИЕ

1. Общият регламент относно защитата на данните (Регламент (ЕС) 2016/679 („ОРЗД“), който влиза в сила на 25 май 2018 г., предвижда една модернизирана и основаваща се на спазването на отчетността и основните права рамка за защитата на данните в Европа. В основата на тази нова рамка са залегнали редица мерки, способстващи за спазването на разпоредбите на ОРЗД. Тези мерки включват задължителни изисквания при конкретни обстоятелства (включително назначаването на длъжностни лица по защита на данните и извършването на оценки на въздействието върху защитата на данните) и доброволни мерки, като кодекси за поведение и механизми за сертифициране.

2. Като част от създаването на механизми за сертифициране и на печати и маркировки за защита на данните в член 43, параграф 1 от ОРЗД се изисква държавите членки да гарантират, че сертифициращите органи, издаващи сертификати по член 42, параграф 1, са акредитирани от компетентния надзорен орган, от националния орган по акредитация или и от двата органа. 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.

3. Подходящите механизми за сертифициране могат да подобрят спазването на ОРЗД и прозрачността спрямо субектите на данни, а също и в търговските отношения между предприятията (B2B), например между администраторите и обработващите лични данни. Администраторите и обработващите лични данни ще се ползват от независима оценка от трета страна, за да докажат съответствието на своите операции по обработване на данни.[1]

4. Във връзка с това Европейският комитет по защита на данните (ЕКЗД) признава, че е необходимо да се предоставят насоки по отношение на акредитацията. Конкретната

[1] В съображение 100 от ОРЗД се казва, че създаването на механизми за сертифициране може да повиши прозрачността и спазването на Регламента и да позволи на субектите на данни да оценяват нивото на защита на данните на съответните продукти и услуги.

стойност и цел на акредитацията се състоят в това, че тя осигурява достоверно становище за компетентността на сертифициращите органи, което позволява да се създаде доверие към механизма за сертифициране.

5. Целта на насоките е да се предоставят инструкции за това как да се тълкуват и прилагат разпоредбите на член 43 от ОРЗД. В частност, те имат за цел да помогнат на държавите членки, надзорните органи и националните органи по акредитация да създадат съгласувана и хармонизирана база за акредитация на сертифициращите органи, които издават сертификати в съответствие с ОРЗД.

2 ПРИЛОЖНО ПОЛЕ НА НАСОКИТЕ

6. В настоящите насоки:

- се определя предназначението на акредитацията в контекста на ОРЗД;
- се обясняват наличните начини за акредитиране на сертифициращи органи в съответствие с член 43, параграф 1, и се определят ключовите въпроси, които трябва да бъдат взети предвид;
- се предоставя рамка за установяване на допълнителни изисквания за акредитация, когато акредитацията се извършва от националния орган по акредитация; както и
- се предоставя рамка за установяване на изисквания за акредитация, когато акредитацията се извършва от надзорния орган.

7. Насоките не са процедурно ръководство за акредитацията на сертифициращите органи в съответствие с ОРЗД. Те не разработват нов технически стандарт за акредитацията на сертифициращите органи за целите на ОРЗД.

8. Насоките са предназначени за:

    - държавите членки, които трябва да гарантират, че сертифициращите органи са акредитирани от надзорния орган и/или от националния орган по акредитация;
    - националните органи по акредитация, които извършват акредитацията на сертифициращи органи съгласно член 43, параграф 1, буква б);
    - компетентния надзорен орган, определящ „допълнителни изисквания“ към тези, посочени в ISO/IEC 17065/2012[2], когато акредитацията се извършва от националния орган по акредитация по смисъла на член 43, параграф 1, буква б);
    - ЕКЗД при издаване на становище относно изискванията за акредитация на компетентните надзорни органи и одобряване на тези изисквания съгласно член 43, параграф 3, член 70, параграф 1, буква п) и член 64, параграф 1, буква в);
    - компетентния надзорен орган, определящ изискванията за акредитация, когато акредитацията се извършва от надзорния орган съгласно член 43, параграф 1, буква а);

[2] Международна организация по стандартизация: Оценка на съответствието — изисквания към органите, сертифициращи продукти, процеси и услуги.

- други заинтересовани страни, като например потенциални сертифициращи органи или собственици на схеми за сертифициране, предлагащи критерии и процедури за сертифициране[3].

9. Определения

10. Чрез следващите определения се цели популяризиране на общо разбиране за основните елементи на процеса на акредитация. Определенията следва да се смятат за отправни точки и нямат претенциите да бъдат неоспорими. Те се основават на съществуващите нормативни уредби и стандарти, по-специално на съответните разпоредби на ОРЗД и ISO/IEC 17065/2012.

11. За целите на настоящите насоки се прилагат следните определения:

12. „*акредитация*“ на сертифициращи органи вж. раздел 3 относно тълкуването на акредитацията за целите на член 43 от ОРЗД;

13. „*допълнителни изисквания*“ означава изискванията, определени от компетентния надзорния орган, спрямо които се извършва акредитацията[4];

14. „*сертифициране*“ означава оценка и безпристрастна атестация от трета страна[5] относно това, че критериите за сертифициране са изпълнени;

15. „*сертифициращ орган*“ означава трета страна — орган[6] за оценяване на съответствието[7], който работи с механизми за сертифициране[8];

16. „*схема за сертифициране*“ означава система за сертифициране, свързана с определени продукти, процеси и услуги, за които важат същите конкретни изисквания, специфични правила и процедури[9];

[3] Собственикът на схемата е разпознаваема организация, която е създала критерии за сертифициране и изисквания, по отношение на които следва да се оцени съответствието. Акредитацията е на организацията, която извършва оценяване (член 43.4) спрямо изискванията на схемата за сертифициране и издава сертификатите (т.е. сертифициращ орган, известен също като орган за оценяване на съответствието). Организацията, извършваща оценяването, може да бъде същата организация, която е разработила схемата и е неин собственик, но може да съществуват договорености, съгласно които една организация да притежава схемата, а друга (или няколко други) да извършва оценяването.

[4] Член 43, параграфи 1, 3 и 6.

[5] Следва да се отбележи, че съгласно ISO 17000, атестацията от трета страна (сертифициране) е „приложима за всички обекти на оценка на съответствието“ (5.5), „с изключение на самите органи за оценяване на съответствието, за които се прилага акредитацията“ (5.6).

[6] Вж. ISO 17000, параграф 2.5: „орган, извършващ услуги по оценяване на съответствието“; ISO 17011: „орган, извършващ услуги по оценяване на съответствието, който може да бъде обект на акредитация“; ISO 17065, 3.12.

[7] Дейността на трета страна по оценяване на съответствието се извършва от организация, която е независима от лицето или организацията, предоставящи обекта, и от потребителските интереси по отношение на този обект, вж. ISO 17000, 2.4.

[8] Член 42.1 и член 42.5 от ОРЗД.

[9] Вж. 3.9 във връзка с приложение Б към ISO 17065.

17. критерии за сертифициране или „критерии“ означава критериите, по които се сертифицира (се оценява съответствието)[10];

18. „национален орган по акредитация“ означава единственият орган в държава членка, който е посочен в съответствие с Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета да извършва акредитация чрез пълномощие, предоставено от държавата[11].

3 ТЪЛКУВАНЕ НА ПОНЯТИЕТО „АКРЕДИТАЦИЯ“ ЗА ЦЕЛИТЕ НА ЧЛЕН 43 ОТ ОРЗД

19. В ОРЗД не се определя понятието „акредитация“. В член 2, параграф 10 от Регламент (ЕО) № 765/2008, с който се определят общи изисквания за акредитациите, акредитация се определя като:

20. „атестация от национален орган по акредитация за това, че съответният орган за оценяване на съответствието отговаря на изискванията, определени в хармонизирани стандарти, и, където е приложимо, всякакви допълнителни изисквания, включително определените в приложимите секторни схеми, да изпълнява специфична дейност по оценяване на съответствието“.

21. Съгласно ISO/IEC 17011

22. „акредитация означава атестация от трета страна по отношение на орган за оценяване на съответствието, представляваща официално доказателство за компетентността му да изпълнява специфични задачи по оценяване на съответствието“.

23. В член 43, параграф 1 се казва:

24. „Без да се засягат задачите и правомощията на компетентния надзорен орган съгласно членове 57 и 58, сертифициращите органи, притежаващи подходящ опит в областта на защитата на данните, след уведомяване на надзорния орган с цел, ако е необходимо, той да може да упражни правомощията си съгласно член 58, параграф 2, буква з), издават и подновяват сертификат. Държавите членки гарантират, че тези сертифициращи органи се акредитират от един или двама от следните органи:

    а) надзорния орган, който е компетентен съгласно член 55 или 56;
    б) националния орган по акредитация, посочен в съответствие с Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета в съответствие с ISO/IEC 17065/2012 и с допълнителните изисквания, определени от надзорния орган, който е компетентен съгласно член 55 или 56“.

25. По отношение на ОРЗД изискванията за акредитация ще се ръководят от:

- ISO/IEC 17065/2012 и „допълнителните изисквания“, определени от надзорния орган, който е компетентен в съответствие с член 43, параграф 1, буква б), когато акредитацията

[10] Вж. член 42, параграф 5.
[11] Вж. член 2.11 от Регламент (ЕО) № 765/2008.

се извършва от националния орган по акредитация и от надзорния орган, когато самият той извършва акредитацията.

26. И в двата случая консолидираните изисквания трябва да обхващат изискванията, посочени в член 43, параграф 2.

27. ЕКЗД приема, че целта на акредитацията е да предостави официално удостоверение за компетентността на органа да извършва сертифициране (дейности по оценяване на съответствието)[12]. Акредитация по смисъла на ОРЗД трябва да се разбира по следния начин:

28. атестация[13] от национален орган по акредитация и/или от надзорен орган за това, че даден сертифициращ орган[14] притежава компетенцията да извършва сертифициране съгласно членове 42 и 43 от ОРЗД, като се вземат предвид ISO/IEC 17065/2012 и с допълнителните изисквания, определени от надзорния орган и/или от Комитета.

4 АКРЕДИТАЦИЯ В СЪОТВЕТСТВИЕ С ЧЛЕН 43, ПАРАГРАФ 1 ОТ ОРЗД

29. В член 43, параграф 1 се признава, че съществуват няколко варианта за акредитация на сертифициращи органи. В ОРЗД се изисква от надзорните органи и държавите членки да определят процедурата за акредитация на сертифициращите органи. В този раздел се определят начините за акредитация, предвидени в член 43.

4.1 Роля на държавите членки

30. В член 43, параграф 1 се изисква от държавите членки *да гарантират*, че сертифициращите органи са акредитирани, но се позволява на всяка държава членка да определя кой следва да отговаря за извършване на оценката, водеща до акредитация. Въз основа на член 43, параграф 1, има три възможности. Акредитацията може да се извършва:

(1) единствено от надзорния орган въз основа на неговите собствени изисквания;
(2) единствено от националния орган по акредитация, посочен в съответствие с Регламент (ЕО) № 765/2008 и въз основа на ISO/IEC 17065/2012 и с допълнителните изисквания, определени от компетентния надзорен орган; или
(3) както от надзорния орган, така и от националния орган по акредитация (и в съответствие с всички изисквания, посочени в точка 2 по-горе).

31. Отделните държави членки трябва да решат дали тези дейности по акредитация ще бъдат извършвани от националния орган по акредитация, от надзорния орган или от

[12] Вж. съображение 15 от Регламент (ЕО) № 765/2008.
[13] Вж. член 2, параграф 10 от Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета от 9 юли 2008 г. за определяне на изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти.
[14] Ср. с определението на понятието „акредитация“ съгласно ISO 17011.

двата органа заедно, но във всеки случай те следва да гарантират, че са предоставени адекватни ресурси[15].

4.2 Взаимодействие с Регламент (ЕО) № 765/2008

32. ЕКЗД отбелязва, че в член 2, параграф 11 от Регламент (ЕО) № 765/2008 се дава определение на национален орган по акредитация като „*единственият* орган в държава членка, който има предоставено от държавата правомощие да извършва акредитация“.

33. Член 2, параграф 11 може да се разглежда като несъвместим с член 43, параграф 1 от ОРЗД, който допуска акредитация от орган, различен от националния орган по акредитация на държавата членка. ЕКЗД счита, че намерението на законодателството на ЕС е да се отклони от общия принцип, че акредитацията се извършва единствено от националния орган по акредитация, като същите правомощия по отношение на акредитацията на сертифициращите органи се предоставят и на надзорните органи. Следователно член 43, параграф 1 е lex specialis по отношение на член 2, параграф 11 от Регламент (ЕО) № 765/2008.

4.3 Роля на националния орган по акредитация

34. В член 43, параграф 1, буква б) се предвижда, че националният орган по акредитация ще акредитира сертифициращи органи в съответствие с ISO/IEC 17065/2012 и с допълнителните изисквания, определени от компетентния надзорен орган.

35. За по-голяма яснота ЕКЗД отбелязва, че конкретното позоваване на параграф 1, буква б), споменато в член 43, параграф 3, означава, че „тези изисквания“ се отнасят до „допълнителните изисквания“, определени от компетентния надзорен орган съгласно член 43, параграф 1, буква б), и изискванията, определени в член 43, параграф 2.

36. В процеса на акредитация националните органи по акредитация следва да прилагат допълнителните изисквания, които трябва да се предоставят от надзорните органи.

37. Сертифициращ орган със съществуваща акредитация въз основа на ISO/IEC 17065/2012 за схеми за сертифициране, различни от свързаните с ОРЗД, който желае да разшири обхвата на своята акредитация, за да включва сертифицирането, извършвано с цел оценка на съответствието с ОРЗД, трябва да отговаря на допълнителните изисквания, определени от надзорния орган, ако акредитацията се извършва от националния орган по акредитация. Ако акредитацията за сертифициране съгласно ОРЗД се извършва само от компетентния надзорен орган, сертифициращият орган, който кандидатства за акредитация, ще трябва да отговаря на изискванията, определени от съответния надзорен орган.

4.4 Роля на надзорния орган

38. ЕКЗД отбелязва, че в член 57, параграф 1, буква р) се предвижда, че надзорният орган *извършва* акредитацията на сертифициращите органи съгласно член 43 като „задача на надзорния орган“ съгласно член 57, а член 58, параграф 3, буква д) предвижда, че надзорният орган има правомощия да дава разрешения и становища да акредитира сертифициращи органи съгласно член 43. Формулировката на член 43, параграф 1 предвижда известна гъвкавост и функцията по акредитация на надзорния орган следва

[15] Вж. член 4, параграф 9 от Регламент (ЕО) № 765/2008.

да се разбира като задача само когато е уместно. За изясняването на този въпрос може да се приложи правото на държавата членка. При все това, в процеса на акредитация от национален орган по акредитация съгласно член 43, параграф 2, буква а) сертифициращият орган трябва да докаже в задоволителна степен своята независимост и опит пред компетентния надзорен орган във връзка с предмета на механизма за сертифициране, който предлага[16].

39. Ако държава членка предвижда сертифициращите органи да бъдат акредитирани от надзорния орган, същият 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 предвиждат по-малко инструкции относно изискванията за акредитация, когато самият надзорен орган извършва акредитацията. С оглед на осигуряването на хармонизиран подход към акредитацията, използваните от надзорния орган критерии за акредитация следва да се ръководят от ISO/IEC 17065 и следва да бъдат допълнени от допълнителни изисквания, определени от надзорния орган в съответствие с член 43, параграф 1, буква б). ЕКЗД отбелязва, че в член 43, параграф 2, букви а)—д) се отразяват и конкретизират изискванията на ISO 17065, което допринася за съгласуваност.

40. Ако държава членка предвижда сертифициращите органи да бъдат акредитирани от националните органи по акредитация, надзорният орган следва да установи допълнителни изисквания, допълващи съществуващите акредитационни конвенции, предвидени в Регламент (ЕО) № 765/2008 (където членове 3—14 се отнасят до организацията и функционирането на акредитацията на органите за оценяване на съответствието), и техническите правила, които описват методите и процедурите на сертифициращите органи. С оглед на това в Регламент (ЕО) № 765/2008 се предвиждат допълнителни насоки. В член 2, параграф 10 е дадено определение на акредитацията и се посочват „хармонизирани стандарти“ и „всякакви допълнителни изисквания, включително определените в приложимите секторни схеми“. От това следва, че допълнителните изисквания, определени от надзорния орган, следва да включват специфични изисквания и да се съсредоточат върху улесняването на оценяването, наред с другото, на независимостта и на нивото на експертния опит в защитата на данните на сертифициращите органи, например на способността им да оценяват и сертифицират операции по обработване на лични данни от администратори и обработващи лични данни съгласно член 42, параграф 1. Това включва компетентностите, необходими за изпълнението на секторни схеми и за защитата на основните права и свободи на физическите лица, и по-специално тяхното право на защита на личните данни[17]. Приложението към настоящите насоки може да спомогне за информирането на компетентните надзорни органи при определянето на „допълнителните изисквания“ в съответствие с член 43, параграф 1, буква б) и член 43, параграф 3.

41. В член 43, параграф 6 се предвижда, че „[и]зискванията, посочени в параграф 3 от настоящия член, и критериите за сертифициране, посочени в член 42, параграф 5, се оповестяват от надзорния орган в леснодостъпна форма“. Следователно с цел

[16] В допълнителните изисквания, определени от надзорния орган съгласно член 43, параграф 1, буква б), следва да се уточнят изискванията за независимост и опит. Вж. също приложение 1 към Насоките.
[17] Член 1, параграф 2 от ОРЗД.

гарантиране на прозрачност, се публикуват всички критерии и изисквания, одобрени от даден надзорен орган. По отношение на качеството и доверието в сертифициращите органи, желателно е всички изисквания за акредитация да бъдат лесно достъпни за обществеността.

4.5 Надзорен орган, действащ като сертифициращ орган

42. В член 42, параграф 5 се предвижда, че даден надзорен орган може да издава сертификати, но в ОРЗД не се изисква той да бъде акредитиран, за да отговаря на изискванията по Регламент (ЕО) № 765/2008. ЕКЗД отбелязва, че с член 43, параграф 1, буква а) и по-специално с член 58, параграф 2, буква з) и параграф 3, букви а), д)—е) се дават пълномощия на надзорните органи да извършват акредитиране и сертифициране и в същото време да дават становища и, когато е приложимо, да отнемат сертификати или да разпореждат на сертифициращите органи да не издават сертификати.

43. Възможни са ситуации, при които разделянето на функциите и задълженията по акредитиране и сертифициране е уместно или необходимо, например ако в дадена държава членка съществуват едновременно надзорен орган и други сертифициращи органи, като и двата вида органи издават сертификати с еднакво приложно поле. Поради това надзорните органи следва да предприемат достатъчно организационни мерки за разделяне на задачите по ОРЗД с цел утвърждаване и улесняване на механизмите за сертифициране, като в същото време вземат предпазни мерки, за да се избегнат конфликтите на интереси, които могат да възникнат от тези задачи. Освен това държавите членки и надзорните органи следва да имат предвид хармонизираното европейско равнище при изготвянето на национално законодателство и процедури, свързани с акредитирането и сертифицирането в съответствие с ОРЗД.

4.6 Изисквания за акредитиране

44. Приложението към настоящите насоки съдържа указания как да се определят допълнителни изисквания за акредитиране. В него се посочват съответните разпоредби от ОРЗД и се предлагат изисквания, които надзорните органи и националните органи по акредитация следва да имат предвид, за да гарантират спазването на ОРЗД.

45. Както е посочено по-горе, когато сертифициращите органи са акредитирани от националния орган по акредитация в съответствие с Регламент (ЕО) № 765/2008, за съответен акредитационен стандарт служи ISO/IEC 17065/2012, разширен с допълнителните изисквания, определени от надзорния орган. В член 43, параграф 2 са отразени общите разпоредби на ISO/IEC 17065/2012 от гледна точка на защитата на основните права съгласно ОРЗД. В приложението член 43, параграф 2 и ISO/IEC 17065/2012 са използвани като основа за установяване на изискванията, както и на допълнителни критерии относно оценяването на експертния опит на сертифициращите органи в областта на защитата на данните и на тяхната способност да зачитат правата и свободите на физическите лица по отношение на обработването на лични данни, както е заложено в ОРЗД. ЕКЗД отбелязва, че се обръща специално внимание на това да се гарантира, че сертифициращите органи имат подходящ опит в областта на защитата на данните в съответствие с член 43, параграф 1.

46. Допълнителните изисквания за акредитиране, определени от надзорния орган, ще се прилагат за всички сертифициращи органи, които са поискали акредитация. Акредитиращият орган ще направи оценка дали конкретният сертифициращ орган е компетентен да изпълнява дейностите по сертифициране в съответствие с

допълнителните изисквания и предмета на сертифицирането. Трябва да се посочат препратки към конкретни сектори или области на сертифициране, за които сертифициращият орган се акредитира.

47. ЕКЗД също така отбелязва, че специален опит в областта на защитата на данни също се изисква, в допълнение към изискванията на ISO/IEC 17065/2012, ако други външни органи, като например лаборатории или одитори, изпълняват части или компоненти от дейностите по сертифициране от името на акредитиран сертифициращ орган. В тези случаи акредитирането на тези външни органи съгласно ОРЗД не е възможно. Въпреки това, за да се гарантира пригодността на тези органи за тяхната дейност, осъществявана от името на акредитираните сертифициращи органи, е необходимо акредитираният сертифициращ орган да гарантира, че опитът по отношение на защитата на данните, необходим за самия акредитиран орган, е наличен и доказан и при външния орган, що се касае до съответната извършвана дейност.

48. Рамката за определяне на допълнителните изисквания за акредитация, представена в приложението към настоящите насоки, не представлява процедурно ръководство за процеса на акредитиране, провеждан от националния орган по акредитация или от надзорния орган. В нея се предоставят насоки относно структурата и методиката, т.е. инструментариум за надзорните органи при определянето на допълнителните изисквания за акредитация.

ПРИЛОЖЕНИЕ 1

Приложение 1 дава насоки за определянето на „допълнителни“ изисквания за акредитация по ISO/IEC 17065/2012 и в съответствие с член 43, параграф 1, буква б) и член 43, параграф 3 от ОРЗД.

В настоящото приложение са посочени примерни изисквания, с които даден надзорен орган по защита на данните следва да се съобрази и които се прилагат по време на акредитацията на сертифициращ орган от националния орган по акредитация или от компетентния надзорен орган[18]. Тези допълнителни изисквания трябва да бъдат съобщени на Европейския комитет по защита на данните преди получаване на одобрение съгласно член 64, параграф 1, буква в).

Това приложение е изготвено във връзка с ISO/IEC 17065/2012. Номерацията на разделите, използвана в настоящото приложение, съответства на тази, използвана в ISO/IEC 17065/2012. Когато надзорните органи извършват акредитация съгласно член 43, параграф 1, буква а), добра практика би било да се следва този подход, когато е уместно. Това ще подпомогне хармонизираната акредитация в ЕС.

Независимо от следващите насоки или от липсата на насоки за всяка точка на ISO/IEC 17065/2012, компетентният надзорен орган може да формулира допълнителни изисквания по отношение на тези точки съгласно националното законодателство.

0 УВОД

[Този раздел включва всички договорени условия за сътрудничество, ако са приложими, между националния орган по акредитация и надзорния орган по защита на данните, например, кой следва да бъде отговорен за получаването на заявления или как да се организира удостоверяването на одобрени критерии като част от процеса на акредитация.]

1 ПРИЛОЖНО ПОЛЕ[19]

Приложното поле на ISO/IEC 17065/2012 се прилага в съответствие с ОРЗД. Насоките за акредитация и сертифициране дават допълнителна информация. Приложното поле на механизма за сертифициране (например, сертифицирането на операции по обработване на данни при използване на облачни услуги) следва да бъде взето под внимание при оценката от страна на националния орган по акредитация (НОА) и компетентния надзорен орган по време на процеса на акредитация, особено във връзка с критериите, опита и методиката за оценка. Широкият обхват на ISO/IEC 17065/2012, включващ продукти, процеси и услуги, не следва да стеснява или да отменя изискванията на ОРЗД, например механизмът за управление не може да бъде единствен елемент от механизма за сертифициране, тъй като сертифицирането трябва да включва обработката на лични данни, т.е. операциите по обработване. Съгласно член 42, параграф 1 от ОРЗД, сертифициране се прилага единствено за операциите по обработване, извършвани от администратори и обработващи лични данни.

[18] За информация относно процеса на одобряване на критериите за сертифициране вж. раздел 4 от насоките за сертифициране.
[19] Номерацията се позовава на ISO/IEC 17065/2012.

2 ПОЗОВАВАНЕ НА НОРМАТИВНА УРЕДБА

ОРЗД има предимство пред ISO/IEC 17065/2012. Ако в допълнителните изисквания или чрез механизъм за сертифициране се прави позоваване на други стандарти на ISO, те трябва да бъдат тълкувани в съответствие с изискванията, определени в ОРЗД.

3 ТЕРМИНИ И ОПРЕДЕЛЕНИЯ

В контекста на настоящото приложение, термините и определенията на насоките относно акредитацията (WP 261) и сертифицирането (ЕКЗД 1/2018) се прилагат и имат предимство пред определенията на ISO.

4 ОБЩИ ИЗИСКВАНИЯ ЗА АКРЕДИТАЦИЯ

4.1 Правни и договорни въпроси

4.1.1 Правна отговорност

Сертифициращият орган трябва да може да докаже (по всяко време) на националния орган по акредитация (НОА) или компетентния надзорен орган (КНО), че той използва актуализирани процедури, съответстващи на правните задължения, определени в условията за акредитация, включително допълнителните изисквания по отношение на прилагането на Регламент (ЕО) 2016/679. Следва да се отбележи, че тъй като самият сертифициращ орган е администратор/обработващ лични данни, той трябва да е в състояние да докаже, че като част от процеса на сертифициране, са въведени процедури и мерки, съответстващи на Регламент (ЕО) 2016/679, особено що се отнася до контрола и обработката на личните данни на организацията на клиента.

КНО може да реши да добави допълнителни изисквания и процедури за проверка на съответствието на сертифициращите органи с ОРЗД преди акредитацията.

4.1.2 Споразумение за сертифициране

Към минималните изисквания към споразумението за сертифициране се добавят следните точки.

Сертифициращият орган трябва да докаже в допълнение към изискванията на ISO/IEC 17065/2012, че неговите споразумения за сертифициране:

1. изискват от заявителя винаги да спазва общите изисквания за сертифициране по смисъла на 4.1.2.2, буква а) от ISO/IEC 17065/2012 и критериите, одобрени от компетентния надзорен орган или ЕКЗД в съответствие с член 43, параграф 2, буква б) и член 42, параграф 5;
2. изискват от заявителя да позволи пълна прозрачност пред компетентния надзорен орган във връзка с процедурата за сертифициране, включително по въпроси, които са поверителни, и са свързани със спазването на защитата на личните данни съгласно член 42, параграф 7 и член 58, параграф 1, буква в);
3. не намаляват отговорността на заявителя да спазва Регламент (ЕО) 2016/679 и не засягат задачите и правомощията на надзорните органи, които са компетентни в съответствие с член 42, параграф 5;

4. изискват от заявителя да предостави на сертифициращия орган цялата информация и достъп до своите дейности по обработване, което е необходимо за извършване на процедурата по сертифициране съгласно член 42, параграф 6;
5. изискват от заявителя да спазва приложимите срокове и процедури. В споразумението за сертифициране трябва да се предвижда, че сроковете и процедурите, произтичащи, например, от програмата за сертифициране или други нормативни актове, трябва да се съблюдават и спазват;
6. по отношение на 4.1.2.2, буква в) № 1 от ISO/IEC 17065/2012, определят правилата за валидност, подновяване и оттегляне по силата на член 42, параграф 7 и член 43, параграф 4, включително правила, определящи подходящи интервали за повторна оценка или преразглеждане (редовност) в съответствие с член 42, параграф 7;
7. позволяват на сертифициращия орган да оповестява цялата информация, необходима за сертифицирането съгласно член 42, параграф 8 и член 43, параграф 5;
8. включват правила относно необходимите предпазни мерки за разследване на жалби по смисъла на 4.1.2.2, буква в) № 2, допълнително буква й) и също така съдържат изрични изявления относно структурата и процедурата за управление на жалби в съответствие с член 43, параграф 2, буква г);
9. в допълнение към минималните изисквания, посочени в 4.1.2.2 от ISO/IEC 17065/2012, ако последиците от оттеглянето или временното прекратяване на акредитацията на сертифициращия орган имат въздействие върху клиента, в този случай, последиците за клиента също следва да бъдат разгледани;
10. изискват от заявителя да информира сертифициращия орган в случай на значителни промени в своето действително или правно положение и в своите продукти, процеси и услуги, обхванати от сертифицирането.

4.1.3 Използване на печати и маркировки за защита на данните

Сертификатите, печатите и маркировките се използват само в съответствие с член 42 и член 43 и с насоките относно акредитация и сертифициране.

4.2 Управление на безпристрастността

Акредитиращият орган гарантира, че в допълнение към изискването по точка 4.2. от ISO/IEC 17065/2012

1. сертифициращият орган ще спазва допълнителните изисквания на компетентния надзорен орган (съгласно член 43, параграф 1, буква б)
    - **а.** ще осигурява отделно доказателство за своята независимост в съответствие с член 43, параграф 2, буква а). Това се отнася, в частност, до доказателствата, свързани с финансирането на сертифициращия орган, в частта, отнасяща се до гарантирането на безпристрастност;
    - **б.** неговите задачи и задължения не водят до конфликт на интереси съгласно член 43, параграф 2, буква д);
2. сертифициращият орган няма съответните взаимоотношения с клиента, когото оценява.

4.3 Отговорност и финансиране

Акредитиращият орган трябва в допълнение към изискването по точка 4.3.1 от ISO/IEC 17065/2012 редовно да гарантира, че сертифициращият орган разполага с подходящи мерки

(напр. застраховки или резерви), за да покрива задълженията си в географските региони, в които осъществява дейност.

4.4 Недискриминационни условия

Надзорният орган може да формулира допълнителни изисквания, ако те съответстват на националното законодателство.

4.5 Поверителност

Надзорният орган може да формулира допълнителни изисквания, ако те съответстват на националното законодателство.

4.6 Общественодостъпна информация

Акредитиращият орган трябва в допълнение към изискването в точка 4.6 от ISO/IEC 17065/2012 да изиска от сертифициращия орган минимум следното:

1. всички версии (текущи и предходни) на одобрените критерии, използвани по смисъла на член 42, параграф 5, да се публикуват и да са лесно, и общественодостъпни, също както, и всички процедури по сертифициране, като се посочва съответният срок на валидност;
2. информацията относно процедурите за обработка на жалби и обжалвания да се оповести публично в съответствие с член 43, параграф 2, буква г).

5 СТРУКТУРНИ ИЗИСКВАНИЯ, ЧЛЕН 43, ПАРАГРАФ 4 [„ПРАВИЛНА“ ОЦЕНКА]

5.1 Организационна структура и висше ръководство

Надзорният орган може да формулира допълнителни изисквания.

5.2 Механизми за осигуряване на безпристрастността

Надзорният орган може да формулира допълнителни изисквания.

6 ИЗИСКВАНИЯ ПО ОТНОШЕНИЕ НА РЕСУРСИТЕ

6.1 Персонал на сертифициращия орган

Акредитиращият орган трябва в допълнение към изискването в раздел 6 от ISO/IEC 17065/2012 да гарантира за всеки сертифициращ орган, че персоналът на последния:

1. доказано притежава подходящи и актуални експертни познания (знания и опит) по отношение на защитата на данни съгласно член 43, параграф 1;
2. е независим и притежава актуални експертни познания във връзка с предмета на сертифицирането в съответствие с член 43, параграф 2, буква а) и няма конфликт на интереси съгласно член 43, параграф 2, буква д);
3. се задължава да спазва критериите, посочени в член 42, параграф 5, в съответствие с член 43, параграф 2, буква б);
4. има подходящи и достатъчни познания и опит в прилагането на законодателството за защита на данните;

5. има подходящи и достатъчни познания и опит в техническите и организационните мерки относно защитата на данните, ако е приложимо;
6. е в състояние да докаже опит в областите, посочени в допълнителните изисквания 6.1.1, 6.1.4 и по-специално 6.1.5.

За персонала с технически експертен опит:

- Да има квалификация в съответната област на технически познания най-малко на ниво 6 по ЕКР[20] или призната защитена степен (напр. дипл. инж.) по съответната регламентирана професия или да има значителен професионален опит.
- *Персоналът, отговарящ за решенията относно сертифицирането,* трябва да притежава значителен професионален опит в определянето и прилагането на мерки за защита на данните.
- *Персоналът, отговорен за оценките,* трябва да притежава професионален опит в техническата защита на данните и познания, и опит в сходни процедури (напр. сертифициране/одити) и да бъде регистриран по надлежния ред.

Персоналът трябва да докаже, че поддържа специфичните за областта познания в техническата сфера и одитните си способности чрез непрекъснато професионално развитие.

За персонала с правен експертен опит:

- Юридическо обучение в университет от ЕС или в признат от държавата университет в продължение на най-малко осем семестъра, включително академичната степен магистър (LL.M. — магистър по право) или еквивалентна степен или значителен професионален опит.
- *Персоналът, който отговаря за решенията относно сертифицирането,* трябва да притежава значителен професионален опит в областта на законодателството за защита на данните и да бъде регистриран според изискванията на държавата членка.
- *Персоналът, отговорен за оценките,* трябва да докаже най-малко две години професионален опит в законодателството за защита на данните и познания и опит в сходни процедури (напр. сертифициране/одити) и, когато това се изисква от държавата членка, да има регистрация.
    - Персоналът трябва да докаже, че поддържа специфичните за областта познания в техническата сфера и одитните си способности чрез непрекъснато професионално развитие.

6.2 Ресурси за оценяване

Надзорният орган може да формулира допълнителни изисквания, ако те съответстват на националното законодателство.

7 ИЗИСКВАНИЯ КЪМ ПРОЦЕСИТЕ, ЧЛЕН 43, ПАРАГРАФ 2, БУКВИ В) И Г)

7.1 Общи положения

[20] Вж. инструмента за сравнение по квалификационната рамка на адрес: https://ec.europa.eu/ploteus/en/compare?

Акредитиращият орган трябва в допълнение към изискването в раздел 7.1 на ISO/IEC 17065/2012 да гарантира следното:

1. Сертифициращите органи отговарят на допълнителните изисквания на компетентния надзорен орган (съгласно член 43, параграф 1, буква б) при подаване на заявлението, така че задачите и задълженията да не водят до конфликт на интереси съгласно член 43, параграф 2, буква б);
2. Уведомяват съответните КНО, преди даден сертифициращ орган да започне да използва одобрен европейски печат за защита на данните в нова държава членка от сателитен офис.

7.2 Заявление

В допълнение към точка 7.2 от ISO/IEC 17065/2012 трябва да се изисква следното:

1. предметът на сертифицирането (обект на оценката, ОнО) трябва да бъде подробно описан в заявлението. Това включва също така интерфейси и прехвърляния към други системи и организации, протоколи, и други гаранции;
2. в заявлението се посочва дали се използват обработващи лични данни, а когато обработващите лични данни са заявители, техните отговорности и задачи трябва да бъдат описани, и заявлението трябва да съдържа съответните договори между администратора, и обработващия лични данни.

7.3 Преглед на заявлението

В допълнение към точка 7.3 от ISO/IEC 17065/2012 трябва да се изисква следното:

1. в споразумението за сертифициране се определят задължителни методи за оценка във връзка с обекта на оценката (ОнО);
2. оценката от 7.3, буква д) относно това дали са налични достатъчни експертни познания, взема предвид в подходяща степен техническия и правния експертен опит в областта на защитата на данните.

7.4 Оценка

В допълнение към точка 7.4 от ISO/IEC 17065/2012 в механизмите за сертифициране трябва да се опишат достатъчно ясно методите за оценка на съответствието на операциите по обработване с критериите за сертифициране, включително, например, когато това е приложимо:

1. метод за оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите им и съответните субекти на данни;
2. метод за оценка на обхвата, състава и всички рискове, отчетени от администратора и обработващия лични данни по отношение на правните последици, произтичащи от членове 30, 32, 35 и 36 от ОРЗД, както и по отношение на определението за технически и организационни мерки съгласно членове 24, 25 и 32 от ОРЗД, доколкото посочените членове се прилагат спрямо предмета на сертифицирането, както и
3. метод за оценяване на коригиращите мерки, включително гаранции, предпазни мерки и процедури, предназначени да се гарантира защитата на личните данни в контекста на обработването, свързано с предмета на сертифицирането, и да се докаже, че са изпълнени законовите изисквания, заложени в критериите; както и
4. документиране на методите и констатациите.

От сертифициращия орган трябва да се изисква да гарантира, че тези методи за оценка са стандартизирани и общоприложими. Това означава, че съпоставими методи за оценка се

използват за съпоставими обекти на оценка. Всяко отклонение от тази процедура трябва да бъде обосновано от сертифициращия орган.

В допълнение към точка 7.4.2 от ISO/IEC 17065/2012 следва да се разреши извършването на оценката от външни експерти, които са признати от сертифициращия орган.

В допълнение към точка 7.4.5 от ISO/IEC 17065/2012 трябва да се изисква сертифицирането за защита на данните в съответствие с членове 42 и 43 от ОРЗД, което вече обхваща част от предмета на сертифицирането, да може да бъде включено в текущото сертифициране. Това обаче няма да бъде достатъчно, за да се заместят напълно (частичните) оценки. Сертифициращият орган е длъжен да проверява спазването на критериите. Признаването винаги изисква наличието на пълен доклад за оценка или информация, позволяваща оценяването на предишни дейности по сертифициране и резултатите от тях. Декларацията за сертифициране или подобни сертификационни документи не може да се считат за достатъчни, за да заменят доклада.

В допълнение към точка 7.4.6 от ISO/IEC 17065/2012 трябва да се изисква сертифициращият орган да посочи подробно в своя механизъм за сертифициране по какъв начин информацията, изисквана в точка 7.4.6, осведомява клиента (заявителя на сертифицирането) относно несъответствията с механизма за сертифициране. Във връзка с това следва да бъдат определени най-малко естеството и момента на подаване на подобна информация.

В допълнение към точка 7.4.9 от ISO/IEC 17065/2012 трябва да се изисква предоставянето на пълен достъп до тази документация на надзорния орган по защита на данните при поискване.

7.5 Преглед

В допълнение към точка 7.5 от ISO/IEC 17065/2012 са необходими процедури за предоставяне, редовно преглеждане и анулиране на съответните сертификати в съответствие с член 43, параграф 2 и член 43, параграф 3.

7.6 Решение относно сертифицирането

В допълнение към точка 7.6.1 от ISO/IEC 17065/2012 от сертифициращия орган трябва да се изиска да изложи подробно в своите процедури как се гарантират неговата независимост и отговорност по отношение на отделните решения относно сертифицирането.

7.7 Документация за сертифициране

В допълнение към точка 7.7.1, буква д) от ISO/IEC 17065/2012 и в съответствие с член 42, параграф 7 от ОРЗД трябва да се изисква срокът на валидност на сертификатите да не надвишава три години.

В допълнение към точка 7.7.1, буква д) от ISO/IEC 17065/2012 трябва да се изисква да бъде документиран и периодът на планираното наблюдение по смисъла на раздел 7.9.

В допълнение към точка 7.7.1., буква е) от ISO/IEC 17065/2012 от сертифициращия орган трябва да се изисква да посочи предмета на сертифицирането в документацията по сертифицирането (като посочи статута на версията или сходни характеристики, ако това е приложимо).

7.8 Указател на сертифицираните продукти

В допълнение към точка 7.8 от ISO/IEC 17065/2012 от сертифициращия орган трябва да се изисква да поддържа вътрешен и публичен достъп до информацията за сертифицираните продукти, процеси и услуги. Сертифициращият орган ще предостави на обществеността резюме

на доклада за оценка. Целта на това резюме е да се подпомогне създаването на прозрачност около това какво е сертифицирано и как е било оценено. Това ще обясни следното:

а) обхвата на сертифицирането и подходящо описание на предмета на сертифицирането (ОнО);

б) съответните критерии за сертифициране (включително версията и функционалния статус);

в) методите за оценка и проведените тестове и

г) резултатите.

В допълнение към точка 7.8 от ISO/IEC 17065/2012 и съгласно член 43, параграф 5 от ОРЗД сертифициращият орган информира компетентните надзорни органи за мотивите за издаване или отнемане на заявения сертификат.

7.9 Надзор

В допълнение към точки 7.9.1, 7.9.2 и 7.9.3 от ISO/IEC 17065/2012 и съгласно член 43, параграф 2, буква в) от ОРЗД трябва да се изисква мерките за редовно наблюдение да бъдат задължителни с цел да се поддържа сертифицирането по време на периода на наблюдение.

7.10 Промени, засягащи сертифицирането

В допълнение към точки 7.10.1 и 7.10.2 от EN ISO/IEC 17065/2012 промените, засягащи сертифицирането, които сертифициращият орган трябва да има предвид, включват: изменения на законодателството за защита на данните, приемане на делегирани актове на Европейската комисия в съответствие с член 43, параграф 8 и член 43, параграф 9, решения на Европейския комитет по защита на данните и съдебни решения, свързани със защитата на данните. Процедурите за промяна, които следва да бъдат договорени тук, може да включват следното: преходни периоди, процес на одобрение от страна на компетентния надзорен орган, преоценка на съответния предмет на сертифициране и подходящи мерки за анулиране на сертификата, ако сертифицираната операция по обработване вече не съответства на актуализираните критерии.

7.11 Прекратяване, ограничаване, временно прекратяване или оттегляне на сертификата

В допълнение към точка 7.11.1 от ISO/IEC 17065/2012 сертифициращият орган трябва да уведоми компетентния надзорен орган и НОА, по целесъобразност, незабавно в писмен вид относно предприетите мерки и относно продължаването, ограниченията, временното прекратяване и оттеглянето на даден сертификат.

Съгласно член 58, параграф 2, буква з) от сертифициращия орган се изисква да приема решения и заповеди от компетентния надзорен орган да оттегли или да не издава сертификат на клиент (заявител), ако изискванията за сертифицирането не са спазени или вече не се спазват.

7.12 Записи

От сертифициращия орган трябва да се изисква да съхранява цялата документация в пълен, разбираем, актуален и подходящ за извършване на одит вид.

7.13 Оплаквания и обжалвания, член 43, параграф 2, буква г)

В допълнение към точка 7.13.1 от ISO/IEC 17065/2012 от сертифициращия орган трябва да се изисква да определи следното:

а) кой може да подава жалби или възражения,

б) кой ги обработва от страна на сертифициращия орган,

в) какви проверки се извършват в този контекст, както и

г) възможностите за консултация със заинтересованите страни.

В допълнение към точка 7.13.2 от ISO/IEC 17065/2012 от сертифициращия орган трябва да се изисква да определи следното:

а) как и на кого трябва да се даде подобно потвърждение,

б) какви са сроковете за това, както и

в) кои процеси следва да бъдат започнати след това.

В допълнение към точка 7.13.1 от ISO/IEC 17065/2012 сертифициращият орган трябва да определи как се гарантира разделението между дейностите по сертифициране и обработката на оплаквания и жалби.

8 ИЗИСКВАНИЯ КЪМ СИСТЕМАТА ЗА УПРАВЛЕНИЕ

Общо изискване към системата за управление съгласно глава 8 от ISO/IEC 17065/2012 е изпълнението на всички изисквания от предходните глави в рамките на обхвата на прилагане на механизма за сертифициране от акредитирания сертифициращ орган да бъде документирано, оценено, контролирано и подложено на независимо наблюдение.

Основният принцип на управление е да се определи система, съгласно която целите на управлението се набелязват по един ефективен и ефикасен начин, и по-специално: изпълнението на услугите по сертифициране да протича чрез подходящи спецификации. Това изисква прозрачност и възможност за проверка на изпълнението на изискванията за акредитация от сертифициращия орган и неговото постоянно съответствие.

За тази цел системата за управление трябва да се спре на методика за постигане и контролиране на тези изисквания в съответствие с разпоредбите за защита на данните и за постоянното им проверяване със самия акредитиран орган.

Тези принципи на управление и документираното им прилагане трябва да бъдат прозрачни и да се съобщават от акредитирания сертифициращ орган в съответствие с процедурата по акредитация и съгласно член 58 и след това по искане на надзорния орган по защита на данните по всяко време в хода на разследване под формата на прегледи на защитата на данните съгласно член 58, параграф 1, буква б) или на преглед на сертификатите, издадени в съответствие с член 42, параграф 7 в съответствие с член 58, параграф 1, буква в).

По-конкретно, акредитираният сертифициращ орган трябва да оповестява публично постоянно и непрекъснато какво се сертифицира, на каква основа (или според какви механизми и схеми за сертифициране), какъв е срокът на валидност на сертификатите въз основа на каква рамка и при какви условия (съображение 100).

8.1 Общи изисквания към системата за управление

Компетентният надзорен орган може да посочи и да добави други допълнителни изисквания, ако съответстват на националното законодателство.

8.2 Документация на системата за управление

Компетентният надзорен орган може да посочи и да добави други допълнителни изисквания, ако съответстват на националното законодателство.

8.3 Контрол на документите

Компетентният надзорен орган може да посочи и да добави други допълнителни изисквания, ако съответстват на националното законодателство.

8.4 Контрол на записите

Компетентният надзорен орган може да посочи и да добави други допълнителни изисквания, ако съответстват на националното законодателство.

8.5 Преглед от ръководството

Компетентният надзорен орган може да посочи и да добави други допълнителни изисквания, ако съответстват на националното законодателство.

8.6 Вътрешни одити

Компетентният надзорен орган може да посочи и да добави други допълнителни изисквания, ако съответстват на националното законодателство.

8.7 Коригиращи действия

Компетентният надзорен орган може да посочи и да добави други допълнителни изисквания, ако съответстват на националното законодателство.

8.8 Предпазни действия

Компетентният надзорен орган може да посочи и да добави други допълнителни изисквания, ако съответстват на националното законодателство.

9 ДРУГИ ДОПЪЛНИТЕЛНИ ИЗИСКВАНИЯ21

9.1 Актуализиране на методите за оценяване

Сертифициращият орган определя процедури, насочващи актуализирането на методите за оценка, които да се прилагат в контекста на оценяването съгласно точка 7.4. Актуализирането трябва да се извършва в хода на промените в правната рамка, съответните рискове, достиженията на техническия прогрес и разходите за прилагане на технически и организационни мерки.

9.2 Поддържане на експертните познания

Сертифициращите органи установяват процедури за осигуряване на обучение на своите служители с оглед актуализиране на техните умения, като отчитат промените, изброени в точка 9.1.

9.3 Отговорности и компетенции

9.3.1 Комуникация между сертифициращия орган и неговите клиенти

Следва да бъдат въведени процедури за прилагане на подходящи процедури и структури за комуникация между сертифициращия орган и неговия клиент. Това включва следното:

[21] Компетентният надзорен орган може да посочи и да добави други допълнителни изисквания, ако съответстват на националното законодателство.

1. Поддържане на документация на задачите и отговорностите от акредитирания сертифициращ орган със следните цели:
    a. искания за информация или
    б. да се даде възможност за контакт в случай на оплакване във връзка със сертифицирането.
2. Поддържане на процеса на подаване на заявления с цел
    a. информация относно статуса на заявлението;
    б. оценки от страна на компетентния надзорен орган по отношение на
        i. обратната информация;
        ii. решенията на компетентния надзорен орган.

9.3.2 Документация на дейностите по оценяване

Надзорният орган може да формулира допълнителни изисквания.

9.3.3 Управление на разглеждането на жалби

Разглеждането на жалби се определя като неразделна част от системата за управление, с която в частност се прилагат изискванията по точка 4.1.2.2, буква в), точка 4.1.2.2, буква й), точка 4.6, буква г) и точка 7.13 от ISO/IEC 17065/2012.

Съответните жалби и възражения следва да се съобщават на компетентния надзорен орган.

9.3.4 Управление на процедурата по оттегляне

Процедурите в случай на временно спиране или оттегляне на акредитацията трябва да бъдат интегрирани в системата за управление на сертифициращия орган, включително в уведомленията за клиентите.