Проект!

Наредба относно условията, изискванията и редът за акредитация и отнемане на акредитация на сертифициращ орган, критериите, механизмите и процедурите за сертифициране, печати и маркировки

Глава първа

Общи разпоредби

Чл. 1. Тази наредба урежда условията, изискванията и реда за акредитация и отнемане на акредитация на сертифициращ орган, както и критериите, механизмите и процедурите за сертифициране, печати и маркировки. Процесът по акредитация и отнемане на акредитация на сертифициращ орган се развива по правилата, установени в правните норми на чл. 42, чл. 43, чл. 57, пар. 1, б. „н“ и б. „р“ от Регламент (ЕС) 2016/679; чл. 14 от Закона за защита на личните данни; чл. 25, т. 13, б. „в“, т. 15, т. 16, т. 18, б. „в“ и чл. 26 – 29 от Правилника за дейността на Комисията за защита на личните данни и нейната администрация, както и настоящата наредба.

Чл. 2. Акредитация на сертифициращ орган се издава от Комисията за защита на личните данни (наричана по-нататък „комисията“). Комисията води публичен регистър на акредитираните сертифициращи органи, съгласно чл. 15, ал. 1, т. 2 от Закона за защита на личните данни.

Чл. 3. Комисията има право да отхвърли всяка процедура за оценяване, която е двусмислена или подвеждаща, или има риск да бъде тълкувана погрешно от субектите на данни или от други трети страни, или ако самата процедура за оценяване не е съвместима с обхвата на сертифицирането. Решението за това се мотивира и подлежи на обжалване по реда на Административнопроцесуалния кодекс в 14-дневен срок от получаването му.

Глава втора

Условия, изисквания и ред за акредитация и отнемане на акредитация на сертифициращ орган

Чл. 4. С получаването на акредитация, сертифициращият орган получава правомощие да предоставя сертификат на заявител за сертифициране.

Чл. 5. Акредитацията на сертифициращ орган се извършва въз основа на критериите за акредитиране на сертифициращи органи, съгласно Приложение 1 към настоящата наредба.

Чл. 6. (1) Процедурата по акредитация се инициира с писмено заявление от кандидата за акредитация до комисията, в което се посочва дали кандидатът използва обработващи лични данни, а когато обработващите лични данни са кандидати за акредитация, към заявлението трябва да бъдат приложени съответните договори между администратора и обработващия лични данни.

(2) Към заявлението се прилагат следните документи, необходими за процедурата:

1. Описание на предмета на сертифицирането, на финансовите, човешките и организационните ресурси;

2. Доказателство за възможността за покриване на финансови пасиви от дейността като сертифициращ орган в съответствие с точка 4.3 ISO / IEC 17065:2012, включително доказателство за сключена застраховка „Гражданска отговорност“ за покриване на исковете за щети, произтичащи от дейността като сертифициращ орган, при което застраховката трябва да се поддържа през целия период на действие на акредитацията;

3. При използването на знаци – печати или маркировки за съответствие по смисъла на чл. 42, пар. 2 и чл. 43, пар. 2, б. „в“ от Регламент (ЕС) 2016/679, се прилага изображение на знаците, както и всички печати, маркировки и лога, предвидени във всяка схема за сертифициране, като преди даден сертифициращ орган да започне да използва одобрен европейски печат за защита на данните в нова държава членка, от изнесен офис, уведомява съответния надзорен орган.

4. Когато е приложимо за конкретните администратори/обработващи лични данни, доказателство за съответствие с изискванията на член 43, параграф 2 от Регламент (ЕС) 2016/679 и международния стандарт ISO / IEC 17065:2012.

(3) Ако заявлението за акредитация и приложените документи не са написани на български език, те трябва да бъдат представяни в официален превод на български език.

Чл. 7. В случай на непълнота или нередовност на представените документи, комисията дава указания на заявителя и определя едномесечен срок за отстраняването им.

Чл. 8. (1) Акредитацията се предоставя за срок от пет години с решение на Комисията за защита на личните данни и може да бъде подновена;

(2) Ако кандидатът за получаване на акредитация като сертифициращ орган не отговаря на условията и критериите, посочени в тази наредба, комисията постановява отказ за даване на акредитация с мотивирано решение, което подлежи на обжалване по реда на Административнопроцесуалния кодекс в 14-дневен срок от получаването му;

(3) Комисията се произнася с решение относно предоставянето или отказа от предоставяне на акредитация на кандидата в срок, не по-дълъг от три месеца, считано от датата на подаване на заявлението или отстраняване на нередностите.

Чл. 9. (1) Три месеца преди изтичането на срока на акредитацията, кандидатът за подновяване на акредитацията като сертифициращ орган подава до комисията искане за подновяване на акредитацията.

(2) Към искането се прилагат актуални документи, доказващи изпълнението на изискванията на тази наредба от страна на сертифициращия орган.

(3) Комисията се произнася с мотивирано решение, като отказът за подновяване на акредитацията подлежи на обжалване по реда на Административнопроцесуалния кодекс в 14-дневен срок от получаването му.

Чл. 10. (1) Сертифициращият орган е длъжен да изпълнява решенията и нарежданията на комисията за отнемане или за не издаване на сертификат на клиент, ако не са спазени или впоследствие (след получаване на сертификат) не се спазват изискванията за сертификация;

(2) Сертифициращият орган е длъжен да публикува и да осигури лесен обществен достъп до всички версии (действащи и предходни) на одобрените критерии за сертифициране и на всички процедури по сертифициране, включително съответните схеми за сертифициране.

Чл. 11. (1) През целия срок на валидност на акредитацията, сертифициращият орган подлежи на контрол от страна на комисията, включително и по отношение на реалната възможност за покриване на финансови пасиви от дейността си като сертифициращ орган, които може да настъпят вследствие на вреди и последващо ангажиране на отговорност по съдебен или извънсъдебен ред на територията, на която упражнява дейността си, като този контрол е неделима част от акредитацията и всяко действие на комисията по упражняване на контрола се документира.

(2) Комисията осъществява контролна дейност по отношение на сертифициращия орган и при получени жалби, сигнали, медийни публикации, както и по собствена инициатива.

(3) При констатиране на несъответствие на вече акредитиран сертифициращ орган с условията и критериите на тази наредба, или при установено неприлагане на решенията на комисията, както и при констатиране на нарушение на Регламент (ЕС) 2016/679, на Закона за защита на личните данни и на тази наредба, от страна на същия орган в качеството му на администратор/обработващ лични данни, комисията отнема неговата акредитация със свое решение, което подлежи на обжалване по реда на Административнопроцесуалния кодекс в 14-дневен срок от получаването му.

Чл. 12. За получаване на акредитация като сертифициращ орган могат да кандидатстват само юридически лица, съгласно определението в точка 4.1.1 ISO / IEC 17065:2012, които отговарят на следните изисквания:

1. Сертифициращият орган трябва да извършва своите дейности безпристрастно в съответствие с точка 4.2 ISO / IEC 17065:2012;

2. Сертифициращият орган трябва да отговаря на недискриминационните условия по смисъла на точка 4.4 ISO / IEC 17065:2012;

3. Липса на всякакъв вид икономически и/или договорни отношения между сертифициращия орган и заявителя или притежателя на сертификат (клиента);

4. Сертифициращият орган трябва да докаже, че:

а. неговата организация е структурирана в съответствие с точка 5.1 ISO / IEC 17065:2012 и механизъм в съответствие с точка 5.2 ISO / IEC 17065:2012 е изпълнено;

б. създадена е процедура за вътрешен одит съгласно изискванията на точка 8.6 ISO / IEC 17065:2012;

в. налице са мерки относно превантивни действия съгласно точка 8.6 ISO / IEC 17065:2012;

г. е в състояние да предприема съответните коригиращи мерки в съответствие с точка 8.6 ISO / IEC 17065:2012.

5. Да бъде в състояние да докаже наличието на ефективна политика по предотвратяване на конфликт на интерес чрез представяне на списък от мерки и ясни процедури, които са задължителни за персонала на сертифициращия орган;

6. Сертифициращият орган трябва да е в състояние да гарантира, че има въведени методи за оценяване и че тези методи за оценяване, описани в механизма за сертифициране, са стандартизирани и общоприложими, като всяко отклонение от тези методи за преценка е нужно да бъде обосновано от сертифициращия орган;

7. Сертифициращият орган трябва да разполага с достатъчно човешки ресурси с актуални специализирани познания в следните области, както и да може да докаже това по всяко време:

а. Познаване на законодателството за защита на данните и опит в неговото прилагане, включително технически и организационни мерки и процедури, или достъп до експерт с подобен опит;

б. Познаване на предмета на сертифициране в съответствие с чл. 43, пар. 2, б. „а“ от Регламент (ЕС) 2016/679;

в. Познаване на съответните законови разпоредби за оценяване на съответствието, както и на националните и международни стандарти (по – специално ISO);

г. Познание в хуманитарната, природната, икономическата и други сфери, необходими при извършване на дейностите в процеса на сертифициране, в зависимост от сферата на дейност на заявителя за получаване на сертификат;

д. Специализираните знания на сертифициращия орган не трябва да се подсигуряват само от едно физическо лице;

е. Сертифициращият орган трябва да използва процедури, за да гарантира, че специализираните знания на персонала се актуализират, по – специално като се вземат предвид промените в правната ситуация, рискът за правата и свободите на субектите на данни и напредъка на техниката и технологиите.

Чл. 13. (1) Правната експертиза се доказва с документ за успешно завършване на специалност „Право“ от висше учебно заведение, а хуманитарната, природната, икономическата или друга експертиза – с документ за успешно завършено обучение по съответната специалност от висше учебно заведение.

(2) В случаите, когато степента на висшето образование е придобито в чуждестранно учебно заведение, се прилагат разпоредбите на Наредбата за държавните изисквания за признаване на придобито висше образование и завършени периоди на обучение в чуждестранни висши училища.

(3) Специализираните знания могат да бъдат доказани и под формата на най-малко пет години професионален опит, което осигурява обща техническа експертиза (не се отнася за правната експертиза).

Чл. 14. (1) Сертифициращият орган може да използва външни експерти в конкретни области, но той носи отговорността за вземане на решения.

(2) Представителите в управителните органи и лицата, които вземат окончателното решение при издаването на сертификата, трябва да имат доказан значителен опит в идентифицирането и прилагането на мерки за защита на данните.

(3) Експертните изисквания към оценителите и лицата, вземащи решения, се определят, като се вземат предвид различните задачи, които изпълняват. Оценителите трябва да имат експертен и професионален опит в техническите процедури (напр. одити и сертифициране), докато лицата, вземащи решения, трябва да имат експертен и професионален опит в защитата на личните данни.

Чл. 15. При юридическо прекратяване дейността на сертифициращия орган или при фактическа невъзможност за изпълнение на задълженията му по наблюдение и оценка на съответствието, същият предава цялата надлежна документация на комисията до определяне на друг сертифициращ орган, на когото тази документация се предава с цел довършване на наблюдение и оценка на съответствието до изтичане срока на сертификата.

Глава трета

Процес на сертифициране

Чл. 16. (1) Схемите за сертифициране трябва да имат ясно определен обхват, от описанието на който трябва ясно да се разбира кои дейности са сертифицирани и кои не са, като изискванията, специфичните правила и процедурите трябва да бъдат конкретно определени.

(2) С цел да се гарантира прозрачност спрямо всяка заинтересована страна, включително субектите на данни, схемата за сертифициране трябва да е ясно структурирана и разбираема, така че всеки, който се занимава със схемата, да разбира процеса и критериите за сертифициране.

(3) Сертифициращият орган трябва да управлява схема за сертифициране в съответствие с раздел 7.1 ISO / IEC 17065:2012.

(4) Собственикът на схема за сертифициране трябва да има разработена процедура за управление на актуализациите на критериите за сертифициране. Тази процедура трябва да бъде част от схемата за сертифициране.

Чл. 17. Схемите за сертифициране могат да бъдат насочени към голям набор от различни операции по обработване, извършвани от администратор/обработващ данни, от различни сектори на дейност (обща схема за сертифициране), или да са насочени към специфични операции по обработване, извършвани от администратор/обработващ данни, и/или за конкретен сектор на дейност (специфична схема за сертифициране).

Чл. 18. (1) Критериите за сертифициране трябва да бъдат формулирани по такъв начин, че да са в съответствие със заявените цели.

(2) Критериите за сертифициране трябва да са формулирани по начин, който не оставят възможност за превратно тълкуване и който начин демонстрира еднозначно очаквания резултат.

(3) Критериите трябва, също така, да обхващат всички възможни сценарии, които обичайно могат да се очакват в зависимост от обхвата на схемата.

Чл. 19. Съдържанието на издаваните сертификатите трябва да бъде прозрачно и ясно за субектите на данни и други заинтересовани страни, за да могат те бързо да идентифицират обхвата на сертифицирането.

Чл. 20. (1) Сертифицирането се извършва въз основа на писмено заявление на заявителя за сертифициране до сертифициращия орган.

(2) В съответствие с точка 7.2 от ISO / IEC 17065:2012, сертифициращият орган трябва да определи изискванията към заявлението, което трябва да съдържа цялата информация, необходима за процеса на сертифициране, и във всеки случай най-малко следната информация:

1. Информация за установяване на самоличността на заявителя за сертифициране, включително данни на упълномощените представители на заявителя за сертифициране;

2. Информация за обхвата на исканата сертификация;

3. Информация за всички външни процеси, използвани от заявителя за сертифициране, включително информация за отношения в съответствие с член 26 или член 28 от Регламент (ЕС) 2016/679.

(3) Сертифициращият орган трябва да оцени писменото заявление на заявителя в съответствие с раздел 7.3 ISO / IEC 17065:2012 и да информира заявителя за състоянието на процеса на сертифициране в разумен срок, както и при поискване.

Чл. 21. (1) Ако в процедурата по сертифициране се установи, че сертификатът не може да бъде издаден поради пропуски на заявителя, на последния се дава възможност да отстрани обстоятелствата или причините, свързани с това, в едномесечен срок.

(2) Сертифициращият орган трябва да вземе решение за сертифициране в разумен срок, като крайният срок за произнасяне трябва да бъде посочен в схемата за сертифициране.

Чл. 22 (1) В процеса на извършване на своята дейност сертифициращият орган трябва да отговаря на недискриминационните условия по смисъла на точка 4.4 ISO / IEC 17065:2012.

(2) Сертифициращият орган трябва да публикува цялата информация за програмата за сертифициране по смисъла на раздел 4.6 ISO / IEC 17065:2012 в общодостъпна форма и да я предоставя при поискване.

Чл. 23. (1) Между сертифициращия орган и заявителя за сертифициране трябва да бъде сключено споразумение за сертифициране.

(2) В споразумението за сертифициране, в допълнение към изискванията по смисъла на точка 4.1.2 ISO / IEC 17065:2012, трябва да се посочи следното:

а. Задължението на заявителя да спазва непрекъснато изискванията за сертифициране и сроковете, посочени в него, включително критериите за сертифициране в съответствие с член 42, параграф 5 от Регламент (ЕС) 2016/679;

б. Задължението на заявителя да внесе промени в случай на промяна в изискванията за сертифициране след предоставяне на разумен период от време;

в. Срокът, за който сертификатът се предоставя или удължава, като максималната продължителност от три години трябва да се вземе предвид в съответствие с член 42, параграф 7 от Регламент (ЕС) 2016/679;

г. Условията, при които сертификатът може да бъде удължен или отменен;

д. Сроковете за преоценка на съответствието с изискванията за сертифициране и критериите за сертифициране;

е. Задължението на заявителя да докладва за значителни промени, които могат да повлияят на изпълнението на договорените задължения;

ж. Задълженията на заявителя във връзка с прекратяване, ограничаване, спиране или отнемане на сертифицирането;

з. Задължението на заявителя, след предварително уведомление, да предостави достъп до експлоатационните или производствените съоръжения и проверка на необходимите документи на лицата, на които е поверено сертифицирането на сертифициращия орган, доколкото това е необходимо за проверка на текущото спазване на задълженията, посочени в споразумението за сертифициране;

и. Задължението на заявителя да осигури пълна прозрачност на процеса на сертифициране спрямо комисията, включително поверителни договорни въпроси;

й. Последиците за заявителя, ако акредитацията на сертифициращия орган бъде отменена;

к. Задължения на сертифициращия орган във връзка с оплаквания относно спазването на изискванията за сертифициране, като по-специално създаване на вътрешен каталог от мерки за разглеждане на получените жалби и задължението за документиране и запазване на жалбите и предприетите мерки, както и за продължителността на съхранение, като се вземат предвид принципите за обработване на лични данни по смисъла на Регламент (ЕС) 2016/679;

л. Методите за оценка по отношение на предмета на сертифицирането;

м. Задължението на заявителя да информира сертифициращия орган за всички нарушения на Регламент (ЕС) 2016/679, Закона за защита на личните данни или друго приложимо секторно законодателство по защита на данните, установено от комисията или друг административен или съдебен орган;

н. Задължението на заявителя да информира сертифициращия орган за всички висящи или приключили производства пред комисията срещу заявителя, свързани с обхвата на сертифициране или обекта на оценката, доколкото проверката или надзорните дейности са свързани с целта на оценката.

(3) Сертифициращият орган е задължен по отношение на заявителя да третира получената в резултат на дейността си информация като поверителна по смисъла на раздел 4.5.1 ISO / IEC 17065:2012.

Чл. 24. В случай на промяна в изискванията за сертифициране, породени от промяната в правната ситуация, решения на съд във връзка със защитата на данните, приемането на делегирани актове на Европейската комисия, сертифициращият орган трябва незабавно да уведоми писмено заявителя, съответно клиента, и след предоставяне на разумен срок за прилагане на необходимите промени, да ги преразгледа.

Чл. 25. Сертифициращият орган трябва, в съответствие с изискванията на раздел 7.4 ISO / IEC 17065:2012, да дефинира стандартизирани методи за оценка, които му позволяват да оценява съответствието на операциите по обработване с критериите за сертифициране. В допълнение към изискванията на раздел 7.4.6 ISO / IEC 17065:2012, сертифициращият орган трябва да определи условията за това как заявителя, съответно клиента, се информира за всякакви отклонения от критериите за сертифициране.

Чл. 26. Сертифициращият орган е длъжен да провери съответствието на операциите по обработване на лични данни на заявителя с критериите за сертифициране.

Чл. 27. Сертифициращият орган трябва да оцени цялата информация и резултати, свързани с оценката по смисъла на точка 7.5 ISO / IEC 17065:2012. 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 от Регламент (ЕС) 2016/679.

Чл. 28. Сертифициращият орган трябва да вземе решение по отношение на предоставянето или недопускането на сертификат въз основа на резултатите от оценката и в съответствие с изискванията на т. 7.6 ISO / IEC 17065:2012.

Чл. 29. Възлагането на решението за сертифициране на външни експерти не е разрешено.

Чл. 30. (1) В случай на сертифициране, сертифициращият орган издава на заявителя за сертифициране писмен сертификат, съдържащ следната информация:

1. Име и адрес на сертифициращия орган;
2. Дата, на която сертификатът е издаден или удължен;
3. Обхват на сертифицирането и описание на предмета на сертифицирането, както и срокът, за който е издаден.

(2) В случай, че сертификатът не е издаден, сертифициращият орган трябва да информира писмено заявителя за сертифициране и да изложи съответните причини за това решение.

(3) Сертифициращият орган, при поискване, е задължен да информира комисията за причините за издаване или неиздаване на сертификат.

Чл. 31. (1) В допълнение към писмения сертификат за съответствие, сертифициращият орган може да издаде на клиента знак за съответствие под формата на печат за защита на данните и/или маркировка, при условие че това е предвидено в приложимите критерии за сертифициране.

(2) Сертифициращият орган трябва да провери използването на знаци за съответствие съгласно ал. 1 по смисъла на точка 4.1.3 ISO / IEC 17065:2012. Във всеки случай, знаците за съответствие могат да се използват само съобразно изискванията на член 42 и член 43 от Регламент (ЕС) 2016/679.

Чл. 32. (1) Сертифициращият орган трябва да съхранява списък на издадените сертификати, който в допълнение към изискванията на раздел 7.8 ISO / IEC 17065:2012 съдържа най-малко следната информация:

1. Обхват на сертифицирането и смислено описание на предмета на сертифицирането;

2. съответни критерии за сертифициране;

3. методи за оценка и проведените тестове;

4. резултати от решенията за сертифициране;

(2) Сертифициращият орган документира, публикува и предоставя в подходяща форма информация за сертифицирани операции по обработване и обобщение на процедурите по сертифициране, включително докладите за оценка.

Чл. 33. (1) В съответствие с раздел 7.9 ISO / IEC 17065:2012 сертифициращият орган трябва да осигури подходящи процедури, които да му позволят да следи текущото спазване на изискванията за сертифициране от клиента (процедура за мониторинг). Всички мерки, свързани с процедурите за мониторинг, включително периода на планираното наблюдение, трябва да бъдат документирани.

(2) Сертифициращият орган трябва да съхранява записи в съответствие с точка 7.12 ISO / IEC 17065:2012, за да докаже, че клиентът отговаря на изискванията за сертифициране. На комисията трябва да бъде предоставян достъп до тези записи при поискване.

Чл. 34. (1) В случай на прекратяване, ограничаване, спиране или отнемане на сертификат, сертифициращият орган трябва да отговаря на изискванията на раздел 7.11 ISO / IEC 17065:2012.

(2) Клиентът има задължение да информира в разумен срок сертифициращия орган за потенциални причини за прекратяването, ограничаването, спирането или отнемането на сертификат.

(3) Сертифициращият орган информира комисията за причините за прекратяването, ограничаването, спирането или отнемането на сертификат.

(4) Неприлагането на решения и/или разпореждания на комисията е самостоятелно основание за отнемане или не издаване/не подновяване на сертификат.

Чл. 35. (1) В съответствие с раздел 7.13 ISO / IEC 17065:2012, сертифициращият орган трябва да определи подходящи процедурни насоки за обработка на жалбите, които получава за нарушения или прилагане на изискванията за сертифициране от клиентите, като сертифициращият орган трябва да определи процедури, гарантиращи разграничението между дейностите по сертифициране и тези по обработката на оплаквания и жалби.

(2) Процедурните указания се публикуват по общодостъпен начин след акредитация на сертифициращия орган.

(3) Сертифициращият орган трябва да води регистър на жалбите, които е получил и предприетите мерки, както и трябва да предостави на комисията достъп до тази информация при поискване.

(4) Сертифициращият орган трябва да направи обществено достъпна информацията във връзка с оплаквания относно спазването на изискванията за сертифициране, както и информацията, свързана с жалби за нарушения на сертификати, като в тези случаи не се разкриват лични данни за страните в производството.

Допълнителни разпоредби

§ 1. По смисъла на тази наредба:

1. ISO 17065 означава ISO/IEC 17065/2012.

2. Акредитация означава издаване на документално потвърждение, на база на взето решение от компетентния надзорен орган, след извършен преглед и с което се потвърждава, че изпълнението на специфични изисквания е доказано и акредитираният е компетентен да извършва сертифициране съгласно членове 42 и 43 от Регламент (ЕС) 2016/679, като се вземат предвид ISO/IEC 17065/2012 и допълнителните изисквания, установени от надзорния орган.

3. Допълнителни изисквания означава изискванията, определени от компетентния надзорния орган, спрямо които се извършва акредитацията.

4. Сертифициране означава оценка и безпристрастна атестация от трета независима страна относно това, че критериите за сертифициране са изпълнени.

5. Сертифициращ орган означава трета независима страна – орган за оценяване на съответствието, който работи с механизми за сертифициране.

6. Схема за сертифициране означава система за сертифициране, свързана с определени продукти, процеси и услуги, за които важат същите конкретни изисквания, специфични правила и процедури.

7. Критерии за сертифициране означава критериите, по отношение на които се оценява съответствието.

8. Заявител означава организацията или лицето, които заявяват сертифициране на операциите си по обработване на лични данни.

9. Клиент означава организацията или лицето, което е сертифицирано.

10. Обща схема за сертифициране означава схема за сертифициране, която е насочена към голям набор от различни операции по обработване, извършвани от администратор/обработващ данни от различни сектори на дейност.

11. Специфична схема за сертифициране означава схема за сертифициране, която е насочена към конкретни операции по обработване, извършено от администратор/обработващ данни и/или за конкретен сектор на дейност или използването на специфична технология.

12. Собственикът на схемата за сертификация е юридическото лице, което е установило критерии за сертифициране и изискванията, спрямо които трябва да се оценява съответствието. Юридическото лице, извършващо оценките, може да бъде същото, което е разработило и притежава схемата, но е допустимо, при наличието на договор, едно юридическо лице да притежава схемата, а друго такова (или повече от едно друго) да извършва оценките.

13. Печати и маркировки за защита на данните са знаци, които имат за цел да демонстрират спазването от страна на администраторите и обработващите лични данни изискванията на Регламент (ЕС) 2016/679 и да позволяват на субектите на данни бързо да оценяват нивото на защита на данните на съответните продукти и услуги.

§ 2. Допустимо е механизмът за сертифициране да се използва като инструмент за трансфер съгласно член 42, параграф 2 от Регламент (ЕС) 2016/679, доколкото има за цел да осигури адекватни гаранции за обработването на лични данни, съгласно условията на член 46, параграф 2, буква е) от същия регламент. Сертифицирането трябва да демонстрира наличието на подходящи предпазни мерки, предоставени от администратори или обработващи данни извън Европейския съюз или представляващи международна организация, получаваща данни от администратори или обработващи данни от ЕС, за да предотврати специфичните рискове при прехвърлянето на лични данни.

Преходни и заключителни разпоредби

§ 1. Тази наредба се издава на основание чл. 14, ал. 5 и ал. 6 от Закона за защита на личните данни, във вр. с чл. 42, чл. 43, чл. 57, пар. 1, б. „п“ и „р“ и чл. 58, пар. 3, б. „д“ и „е“ от Регламент (ЕС) 2016/679.

§ 2. Регламент (ЕС) 2016/679 се прилага с предимство пред ISO/IEC 17065/2012 и изискванията на механизма за сертифициране.

§ 3. Неразделна част от тази наредба е Приложение 1 към чл. 5, съдържащо критериите относно условията, изискванията и редът за акредитация и отнемане на акредитация на сертифициращ орган.

§ 4. Дирекция „Правно-аналитична, информационна и контролна дейност“ към комисията следи за актуалните изисквания на ISO/IEC 17065/2012 и при промяна заедно с дирекция „Правно-нормативна и международна дейност“, в рамките на своите функционални компетентности съгласно разпоредбите на Правилника за дейността на Комисията за защита на личните данни и на нейната администрация, предлагат на комисията да внесе съответните изменения в тази наредба.

Приложение № 1 към чл. 5

Критерии за акредитация на сертифициращ орган съгласно член 43, параграф 3 от Регламент (ЕС) 2016/679, приети с решение на комисията от 20.07.2022 г. и във връзка със Становище 13/2022 на ЕКЗД по чл. 64, пар. 1 от Регламент (ЕС) 2016/679

РЕШЕНИЕ НА
КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Българският независим надзорен орган, отговорен за наблюдението на прилагането на Регламент (ЕС) 2016/679 (Общ регламент за защита на данните, наричан по-долу ОРЗД), натоварен със задачата да осигури защита на основните права и свободи на физическите лица във връзка с обработването и свободното движение на лични данни в рамките на Съюза - Комисия за защита на личните данни, наричана по-долу КЗЛД, приема следния документ относно изискванията за акредитация на Сертифициращи органи по отношение на ISO/IEC 17065/2012 в съответствие с член 43 от ОРЗД. Настоящият документ трябва да се тълкува във

връзка с ISO/IEC 17065/2012 и като въвеждащ допълнителни критерии за акредитиране в конкретната материална област.

Увод

Във връзка с процедурата по акредитация на сертифициращи органи в българския Закон за защита на личните данни (ЗЗЛД), и по-конкретно в чл. 14, са установени следните основни положения: КЗЛД извършва акредитация на сертифициращи органи в съответствие с Регламент (ЕС) 2016/679, въз основа на изисквания, определени от нея или от Европейския комитет по защита на данните; акредитацията се издава съгласно чл. 43, параграф 2 от Регламент (ЕС) 2016/679 за срок от 5 години и може да се поднови; КЗЛД отнема акредитацията на сертифициращ орган, когато не са спазени условията за акредитация или когато предприетите от сертифициращия орган действия нарушават този закон или Регламент (ЕС) 2016/679; решенията на КЗЛД за отнемане на акредитация по ал. 3 може да се обжалват по реда на административнопроцесуалния кодекс. Съгласно чл. 14, ал. 5 от ЗЗЛД, КЗЛД има задължение да издаде наредба за условията и реда за акредитация и отнемане на акредитация на сертифициращи органи.

По смисъла на ЗЗЛД КЗЛД има вменено правомощие да издава акредитация на сертифициращ орган, каквато възможност е предвидена в чл. 43, параграф 1, б. „а“ и чл. 58, параграф 3, б. „д“ от ОРЗД. За целта, КЗЛД възнамерява да одобри критериите за акредитиране по на чл. 43, параграф 3 от ОРЗД и да ги предостави на ЕКЗД за становище по чл. 64, параграф 1, б. „в“ от ОРЗД. В националното законодателство не е предвидена функция на националния орган по акредитация в процедурата по акредитация на сертифициращи органи по смисъла на ОРЗД.

КЗЛД има задължение да води публичен регистър на акредитираните сертифициращи органи (чл. 15, ал. 1, т. 2от ЗЗЛД).

Механизмът за сертифициране, по който Сертифициращите органи, акредитирани по реда на ISO/IEC 17065/2012, ще издават и подновяват сертификати, е допълнителен инструмент за доказване на съответствието с ОРЗД при дейностите по обработване на лични данни от администратори/обработващи и по този начин усилията тези лица по спазване на съответствие със стандартите за защита на данните ще получат стандартизирана оценка. ОРЗД се прилага с предимство пред ISO/IEC 17065/2012 и изискванията на механизма за сертифициране.

Настоящите критерии са разработени въз основа на ОРЗД и Насоки 4/2018 на ЕКЗД относно акредитацията на сертифициращи органи съгласно чл. 43 от ОРЗД и ще залегнат като

неразделна част от Наредбата относно условията и реда за акредитация и отнемане на акредитация по чл. 14, ал. 5 от ЗЗЛД.

1 Приложно поле

Приложното поле на механизма за сертифициране в представения проект за решение съдържа допълнителни изисквания към ISO/IEC 17065/2012 за оценка на компетентността, последователната работа и безпристрастността на сертифициращите органи, финансовите, човешките и организационните им ресурси, както и изискване за предоставяне на информация за критериите за сертифициране съгласно член 42, параграф 5 от Регламент (ЕС) 2016/679. Тоест, обхватът на ISO/IEC 17065/2012 не стеснява и не отменя изискванията на ОРЗД, а го допълва и надгражда, но се отнася само до операции по обработване на лични данни от администратор/обработващ.

2 Позоваване на нормативна уредба

При вземане на решение от страна на КЗЛД, в качеството ѝ на компетентен надзорен орган, доколко изпълнението на специфични изисквания е доказано и сертифициращият орган е компетентен да извършва сертифициране, се вземат под внимание изискванията, съдържащи се в правните норми на ОРЗД, и всички позовавания на стандарти на ISO са съобразени с тези изисквания.

3 Термини и определения

За нуждите на предложения проект на решение се използват определенията, съдържащи се в Насоки 4/2018 относно акредитацията на сертифициращи органи съгласно член 43 от ОРЗД, а именно:

1.) Общ регламент относно защитата на данните означава Регламент (ЕС) 2016/679 - ОРЗД;

2.) ISO 17065 означава ISO/IEC 17065/2012;

3.) „Акредитация“ на сертифициращи органи вж. раздел 3 относно тълкуването на акредитацията за целите на член 43 от ОРЗД;

4.) „Допълнителни изисквания“ означава изискванията, определени от компетентния надзорния орган, спрямо които се извършва акредитацията;

5.) „Сертифициране“ означава оценка и безпристрастна атестация от трета страна относно това, че критериите за сертифициране са изпълнени;

6.) „Сертифициращ орган“ означава трета страна — орган6 за оценяване на съответствието , който работи с механизми за сертифициране;„схема за сертифициране“ означава система за сертифициране, свързана с определени продукти, процеси и услуги, за които важат същите конкретни изисквания, специфични правила и процедури;Критерии за сертифициране или

„критерии“ означава критериите, по които се сертифицира (се оценява съответствието);Заявител означава организацията или лицето, които заявяват сертифициране на операциите си по обработване на лични данни;

7.) Клиент означава организацията или лицето, което е сертифицирано.

4 Общи изисквания за акредитация

4.1 Правни и договорни въпроси

4.1.1 Правна отговорност

В проекта на решение е предвидено през целия срок на валидност на акредитацията (5 години), Сертифициращият орган да подлежи на контрол от страна на КЗЛД, като този контрол е неделима част от акредитацията и всяко действие на КЗЛД по упражняване на контрола се документира. КЗЛД осъществява своята контролна дейност по отношение на сертифициращият орган при получени жалби, сигнали, въз основа на обществено достъпна информация и по собствена инициатива. При констатиране на несъответствие на вече акредитиран сертифициращ орган с условията и изискванията на настоящите критерии, както и при констатиране на нарушение на Регламент (ЕС) 2016/679 и Закона за защита на личните данни от страна на същия орган в качеството му на администратор/обработващ лични данни, за КЗЛД е налице правомощие да отнема неговата акредитация със свое решение.

Отговорност на Сертифициращия орган е да в състояние по всяко време да докаже пред КЗЛД, че разполага с актуални процедури, които гарантират съответствие с правните задължения, установени в критериите за акредитация, включително и с мерки, които гарантират по безспорен начин, че обработването на лични данни на Заявителя и Клиента, като част от процеса по сертифициране, са в съответствие с изискванията на ОРЗД. Като елемент от тези мерки се приема предоставянето на доказателство от Сертифициращия орган, че има добра професионална репутация в сферата на защитата на личните данни, част от която е липсата на минали или висящи производства по нарушение на ОРЗД пред КЗЛД или друг компетентен надзорен орган. Наличието на такива производства ще бъде считано за основание за преустановяване на процедурата по акредитиране и евентуално за отнемане на акредитация.

4.1.2 Споразумение за сертифициране

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

1. Заявителят 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 от ОРЗД;

2. Заявителят да позволи пълна прозрачност пред КЗЛД 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) от ОРЗД;

3. да не намаляват отговорността на Заявителя да спазва Регламент (ЕО) 2016/679 и не засягат задачите и правомощията на КЗЛД, които са компетентни в съответствие с член 42, параграф 5 от ОРЗД;

4. Заявителят да предостави на Сертифициращия орган цялата информация и достъп до своите дейности по обработване, необходими за извършване на процедурата по сертифициране съгласно член 42, параграф 6;

5. Заявителят 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 приложими 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 от ОРЗД, включително правила, определящи относимите интервали за повторна оценка или преразглеждане (редовност) в съответствие с член 42, параграф 7 от ОРЗД;

7. позволяват на Сертифициращия орган да предава на КЗЛД цялата необходима информация по процедурата на сертифицирането съгласно член 42, параграф 8 и член 43, параграф 5 от ОРЗД;

8. включват правила относно необходимите мерки за разглеждане на жалби по смисъла на 4.1.2.2, буква в) № 2, допълнително буква й) от ISO/IEC 17065/2012 и също така съдържат изрични разпоредби относно структурата и процедурата за обработване на жалби за нарушение на сертификата в съответствие с член 43, параграф 2, буква г) от ОРЗД;

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 трябва да бъдат разписани;

10. Заявителят да информира сертифициращия орган в случай на значителни промени в своето фактическо или правно положение и в своите продукти, процеси и услуги, обхванати от сертифицирането;

11. Заявителят да информира, извън задълженията му по чл. 33 от ОРЗД, Сертифициращия орган за всички нарушения или съмнения за нарушения на сигурността на данните, които имат или може да имат отражение върху условията за валидност на сертификата;

12. Заявителят да информира Сертифициращия орган за всички нарушения на ОРЗД, ЗЗЛД или друго приложимо секторно законодателство по защита на данните установено от КЗЛД или друг административен орган, или компетентният съд.

4.1.3 Използване на печати и маркировки за защита на данните

За използването на знаци – печати или маркировки, изображение на знаците или лога, предвидени във всяка схема за сертификация, те трябва да са в пълно съответствие с чл. 42, пар. 2 и чл. 43, пар. 2, б. „в“ от Регламент (ЕС) 2016/679 и Насоки 4/2018 на ЕКЗД.

4.2 Управление на безпристрастността

1. Налице е задължението Сертифициращият орган да извършва своите дейности безпристрастно в съответствие с точка 4.2 ISO / IEC 17065: 2012;

2. В съответствие с чл. 43, параграф 2, б. „а“ от ОРЗД, Сертифициращият орган трябва да предостави отделно доказателства за независимо финансиране, които да удостоверяват липса на конфликт на интереси при финансирането.

3. Декларация за липса на всякакъв вид икономически и/или договорни отношения между Сертифициращия орган и Заявителя или Клиента (притежателя на сертификат).

4. Сертифициращият орган трябва да разполага с ефективна политика по предотвратяване на конфликт на интерес чрез представяне на списък от мерки, които са задължителни за персонала на Сертифициращия орган, включително и разделение на процесите в рамките на самия орган с цел избягване на конфликт на интереси.

5. Сертифициращият орган трябва да установи ясни процедури за идентифициране и управление на конфликти на интереси.

6. Уставните правила на Сертифициращият орган трябва да предвиждат независимост на управляващите му органи/управител, които да могат ефективно да се прилагат при изпълнение на Споразумението за сертифициране.

4.3 Отговорност и финансиране

Сертифициращ орган, в съответствие с точка 4.3 ISO / IEC 17065: 2012, трябва да периодично да представя на КЗЛД доказателства за реална възможност за покриване на финансови пасиви от дейността си като Сертифициращ орган, които може да настъпят в следствие на вреди и последващо ангажиране на отговорност по съдебен или извънсъдебен ред на територията, на която упражнява дейността. Такова доказателство, може да бъде генерирането на фонд „Резервен“, сключването на съответната застраховка „професионална“ или „обща“ отговорност или други обезпечителни мерки. Преценката за адекватност на финансирането ще включва и баланс между съотношението на размера и обема дейност на

Сертифициращия орган и размера на съответните финансови гаранции, които представя. Всички тези гаранции трябва да покриват целия период на действие на акредитацията.

4.4 Недискриминационни условия

Сертифициращият орган трябва да отговаря на недискриминационните условия по смисъла на точка 4.4 ISO / IEC 17065: 2012.

4.5 Поверителност

Задължението на Заявителя за сертифициране е да осигури пълна прозрачност на процеса на сертифициране спрямо органа за защита на данните – КЗЛД, включително поверителни договорни въпроси. Сертифициращият орган е задължен по отношение на Заявителя за сертифициране да третира получената в резултат на дейността си информация като поверителна по смисъла на раздел 4.5.1 ISO / IEC 17065: 2012.

4.6 Общественодостъпна информация

В допълнение на изискванията на ISO 17065, Сертифициращият орган трябва да докаже пред КЗЛД, че:

1. публикува на интернет страницата си и е осигурил лесен обществен достъп до всички версии (действащи и предходни) на одобрените критерии за сертифициране и на всички процедури по сертифициране, включително съответните схеми за сертифициране.

2. е обществено достъпна информацията във връзка с оплаквания относно спазването на изискванията за сертифициране, както и информация, свързана с жалби за нарушения на сертификати, включително процедурата за разглеждане на жалби, както и информация относно процедурите по обжалване на жалбите; подсигурил е, по смисъла на чл. 42, параграф 2, б. „г“ от ОРЗД, процедури и структура за обработване на тези сигнали и жалби и по – специално е създавал вътрешен набор от мерки за разглеждане на получените жалби и задължението за документиране и запазване на жалбите и предприетите мерки по тях, които включват и правила за продължителността на съхранение, като се вземат предвид принципите за обработка на лични данни по смисъла на ОРЗД. В тези случаи информация, съдържаща лични данни относно страните по производствата не трябва да бъде разкривана.

3. е публикувал списък със сертифицираните си Клиенти, включително резюме от оценката за сертифициране на всеки от тях, обхвата на сертификата им, относимите към тях критерии за сертифициране, методите за оценка и резултатите от нея.

Доказването на горните изисквания става чрез предоставянето на КЗЛД на разписани процедури за публично оповестяване на информацията по ISO 17065 и допълнителните критерии.

5 Структурни изисквания, член 43, параграф 4 („правилна“ оценка)

5.1 Организационна структура и висше ръководство

За получаване на акредитация като Сертифициращ орган могат да кандидатстват само юридически лица, съгласно определението в точка 4.1.1 ISO / IEC 17065: 2012, които отговарят на съответните изисквания. Сертифициращият орган трябва да докаже, че неговата организация е структурирана в съответствие с точка 5.1 ISO / IEC 17065: 2012 и механизъм в съответствие с точка 5.2 ISO / IEC 17065: 2012.

5.2 Механизми за осигуряване на безпристрастността

Сертифициращият орган трябва да извършва своите дейности безпристрастно в съответствие с точка 4.2 ISO / IEC 17065: 2012. Липса на всякакъв вид икономически и/или договорни отношения между сертифициращия орган и заявителя или притежателя на сертификат е елемент от доказване на безпристрастността.

6. Изисквания по отношение на ресурсите

Сертифициращият орган трябва, в допълнение към изискването в раздел 6 от ISO/IEC 17065/2012, да докаже пред КЗЛД, 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 от ОРЗД;

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) от ОРЗД;

3. се задължава да спазва критериите, посочени в член 42, параграф 5, в съответствие с член 43, параграф 2, буква б) от ОРЗД;

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. представителите в управителните органи и лицата, които вземат окончателното решение при издаването на сертификата, трябва да имат значителен опит в идентифицирането и прилагането на мерки за защита на данните;

7. 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:

Сертифициращият орган трябва да разполага с достатъчно човешки ресурси с актуални специализирани познания в следните области, както и да може да докаже това по всяко време:

Познаване на предмета на сертифициране в съответствие с чл.43, пар. 2, б. „а“ от Регламент (ЕС) 2016/679;

Те са придобили квалификация в съответната област на техническата експертиза или призната образователно-квалификационна степен, както и технически професионален опит в защитата на данните.

Познание в, икономическата, технически или други сфери, необходими при извършване на дейностите в процеса на сертифициране, в зависимост от сферата на дейност на кандидата за получаване на сертификат;

Специализираните познания за лицата, които провеждат оценките за сертифициране, в конкретната област се доказват с относимата за конкретната сфера на познания диплома за завършен цикъл на висше образование и допълнително професионален опит в областта, но не по-малко от три години, които да включват и опит във водене на проверки (одити).

Експертните изисквания към оценителите и лицата, вземащи решения, се определят, като се вземат предвид различните задачи, които изпълняват. Оценителите трябва да имат експертен опит и професионален опит в техническите процедури (напр. одити и сертифициране), докато лицата, вземащи решения, трябва да имат експертен опит и професионален опит в защитата на данните.

Специализираните знания за Сертифициращия орган в цялост не трябва да бъдат гарантирани само от едно физическо лице.

Представителите в ръководните органи и лицата, които взимат окончателното решение за издаване на сертификат, освен горните изисквания трябва да разполагат със значителен професионален опит в сферата на защитата на данните.

Сертифициращият орган трябва да използва процедури, за да гарантира, че специализираните знания на персонала се актуализират, по - специално като се вземат предвид промените в правната ситуация, рискът за обработването на лични данни и състоянието на техниката и технологиите.

Сертифициращият орган може да използва външни експерти в конкретни области, но Сертифициращият орган носи отговорността за вземане на решения. При всички положения, Сертифициращият орган трябва да докаже, че разполага с достатъчен на брой специалисти с оглед предметния обхват и обема на предвижданото сертифициране, за да гарантира съответното ниво на експертна обезпеченост.

За персонала с правен експертен опит:

Познаване на законодателството за защита на данните и опит в неговото прилагане, включително технически и организационни мерки и процедури, или достъп до експерт с подобен опит.

Да притежава удостоверение за юридическа правоспособност от Министерство на правосъдието на Република България, или да бъде регистриран според изискванията на съответната държава членка на ЕС.

Познаване на съответните законови разпоредби за оценяване на съответствието, както и на националните и международни стандарти (по - специално ISO);

Правната експертиза се доказва с документ за успешно завършване на специалност „Право“ от висше учебно заведение със степен магистър;

В случаите, когато степента на висшето образование е придобито в чуждестранно учебно заведение, се прилагат разпоредбите на Наредбата за държавните изисквания за признаване на придобито висше образование и завършени периоди на обучение в чуждестранни висши училища;

Специализираните познания за лицата, които провеждат оценките, трябва да разполагат с реален опит в областта на защитата на данните, но не по-малко от три години, които да включват и опит във водене на проверки (одити).

Представителите в ръководните органи и лицата, които взимат окончателното решение за издаване на сертификат, освен горните изисквания, ако доказват правна експертиза, трябва да разполагат със значителен професионален опит в сферата на защитата на данните.

Сертифициращият орган трябва да използва процедури, за да гарантира, че специализираните знания на персонала се актуализират, по - специално като се вземат предвид промените в правната ситуация, рискът за обработка и състоянието на техниката и технологиите.

Посочените общи изисквания по отношение на ресурсите на сертифициращия орган ще бъдат включени в наредбата за условията и реда за акредитация и отнемане на акредитация на сертифициращи органи, която ще бъде приета въз основа на настоящите критерии.

6.2 Ресурси за оценяване

Прилагат се изискванията на ISO / IEC 17065: 2012.

7 Изисквания към процесите, член 43, параграф 2, букви в) и г)

7.1 Общи положения

1. Сертифициращите органи трябва да 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);

7.2 Заявление

В допълнение на изискванията на ISO / IEC 17065: 2012, Сертифициращият орган ще трябва да изисква Заявлението да съдържа:

1.подробно описание на обекта на оценката (ОнО);

2.посочване 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;

3.посочване дали ще се обработват данни от съвместни администратори и дали съвместния администратор е Заявител, като към Заявлението се прилага и споразумението между съвместните администратори;

4.информация за всички висящи или приключили производства пред КЗЛД срещу Заявителя, свързани с обхвата на сертифициране или обекта на оценката, доколкото разследването или регулаторните действия са свързани с целта на оценката.

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 и да се предоставят на КЗЛД, 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 обекта на оценката, както и

3. метод за оценяване на корективните мерки, включително гаранции, предпазни мерки и процедури, предназначени да се гарантира защитата на личните данни в контекста на обработването, свързано с ОнО, и да се докаже, че са изпълнени законовите изисквания, заложени в критериите; както и

4. документиране на методите и констатациите.

Сертифициращият орган трябва 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 трябва 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 не изключва извършването на 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 трябва 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.

5. Сертифициращият орган трябва да установи процедури по актуализирането на методите за оценка, както е описано в под-раздел 9.1 от тези критерии.

7.5 Преглед

Задължение на Заявителя за сертифициране е да предостави достъп до експлоатационните или производствените съоръжения и проверка на необходимите

документи на лицата, на които е поверено сертифицирането на сертифициращия орган, доколкото това е необходимо за проверка на текущото спазване на задълженията, посочени в споразумението за сертифициране, след предварително уведомление.

В съответствие с раздел 7.9 ISO / IEC 17065: 2012 Сертифициращият орган трябва да осигури подходящи процедури, които да му позволят да следи текущото спазване на изискванията за сертифициране от притежателя на сертификата (процедура за мониторинг). Всички мерки, свързани с процедурите за мониторинг, включително периода на планираното наблюдение, трябва да бъдат документирани, съгласно описани процедури.

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.

Сертифициращият орган трябва да води регистър на жалбите, които е получил и предприетите мерки, както и трябва да предостави на КЗЛД достъп до тях по всяко време.

7.6 Решение относно сертифицирането

Сертифициращият орган трябва да извършва своите дейности безпристрастно в съответствие с точка 4.2 ISO / IEC 17065: 2012, както и да бъде в състояние да докаже наличието на ефективна политика по предотвратяване на конфликт на интерес чрез представяне на списък от мерки, които са задължителни за персонала на сертифициращия орган. Сертифициращият орган трябва да е в състояние да гарантира, че има въведени методи за оценяване и че тези методи за оценяване, описани в механизма за сертифициране, са стандартизирани и общоприложими, като всяко отклонение от тези методи за преценка е нужно да бъде обосновано от сертифициращия орган.

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.

Непосредствено преди издаване на решението, Сертифициращият орган трябва да уведоми КЗЛД за предстоящото решение, като към него представи резюме на същото, включващо описание на спазване на настоящите критерии и основанията за сертифициране, както и декларация, че Заявителят не е в процес на производство пред КЗЛД. При издаване на окончателното решение, Сертифициращият орган го предоставя в цялост на КЗЛД. Същата процедура се следва при подновяване или удължаване на сертифицирането. Това задължение е да осигури честно и прозрачно прилагане на критериите за акредитация във връзка с решенията, издадени от Сертифициращия орган и не представлява форма на надзор от КЗЛД при взимане на решения от страна Сертифициращия орган.

7.7 Документация за сертифициране

Срокът, за който сертификатът се предоставя или удължава, като максималната продължителност е от три години, в съответствие с член 42, параграф 7 от ОРЗД.

В съответствие с раздел 7.9 ISO / IEC 17065: 2012 Сертифициращият орган трябва да осигури подходящи процедури, които да му позволят да следи текущото спазване на изискванията за сертифициране от притежателя на сертификата (процедура за мониторинг). Всички мерки, свързани с процедурите за мониторинг, включително периода на планираното наблюдение, трябва да бъдат документирани.

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).

В случай на сертифициране, Сертифициращият орган издава на Заявителя за сертифициране писмен сертификат, съдържащ:

- информация относно обхвата на сертифицирането;
- описание на предмета на сертифицирането;
- периода на валидност на сертификата;
- името/наименованието и идентифициращи данни на получателя на сертификата.

Тази информация трябва да съвпада напълно с информацията, съдържащата се в решението за сертифициране.

7.8 Указател на сертифицираните продукти

Сертифициращият орган трябва да съхранява списък на издадените сертификати, който в допълнение към изискванията на раздел 7.8 ISO / IEC 17065: 2012 съдържа най -малко следната информация:

1. обхватът на сертифицирането и подходящо описание на предмета на сертифицирането (ОнО);

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

3. методите за оценка и проведените тестове;

4. резултатите от решенията за сертифициране;

Сертифициращият орган е задължен да оповести публично информацията по точки 1 – 4, включително в резюмето.

Сертифициращият орган документира, съхранява, публикува и предоставя в подходяща форма информация за сертифицирани операции по обработване на лични данни и обобщение на процедурите по сертифициране, включително докладите за оценка.

Сертифициращият орган е задължен да информира КЗЛД за причините за издаване или не издаване на сертификат.

7.9 Надзор

В съответствие с раздел 7.9 ISO / IEC 17065: 2012 сертифициращият орган трябва да осигури подходящи процедури, които да му позволят да следи текущото спазване на изискванията за сертифициране от притежателя на сертификата (процедура за мониторинг). Трябва да бъде извършена оценка, за да се гарантира, че процедурата за мониторинг съответства на рисковете, свързани с планираната обработка. Всички мерки, свързани с процедурите за мониторинг, включително периода на планираното наблюдение, трябва да бъдат документирани.

Сертифициращият орган трябва да съхранява записи в съответствие с точка 7.12 ISO / IEC 17065: 2012, за да докаже, че притежателят на сертификата отговаря на изискванията за сертифициране. На КЗЛД трябва да бъде предоставен достъп до тези записи по всяко време.

При юридическо прекратяване дейността на Сертифициращият орган или при фактическа невъзможност за изпълнение на задълженията му по надзор, същият предава цялата надлежна документация на КЗЛД до определяне на друг сертифициращ орган, на когото тази документация се предава с цел довършване на надзора до изтичане срока на сертификата.

7.10 Промени, засягащи сертифицирането

В случай на промяна в изискванията за сертифициране, породени от нарушения на сигурността на данните или нарушения на законодателството в областта на защитата на данните, както и факти и обстоятелства които биха имали трайни неблагоприятни последици за процеса на сертифициране, установени от КЗЛД, съответния административен орган или компетентния съд, и са свързани с предмета на сертифициране, неспазване на настоящите критерии, промяната в законодателството, решения на съд във връзка със защитата на данните, приемането на делегирани актове на Комисията или документи приети от ЕКЗД, Сертифициращият орган трябва незабавно да уведоми писмено притежателя на сертификата, доколкото същият има отношение към процедурата по сертифициране и след предоставяне на разумен срок за прилагане на необходимите промени, да ги преразгледа. За целта Сертифициращият орган трябва да разработи съответната процедура (напр. периодичен преглед на законодателството и съдебната практика в областта на защитата на данните, процес на одобрение с компетентния надзорен орган).

7.11 Прекратяване, ограничаване, временно прекратяване или оттегляне на сертификата

В случай на прекратяване, ограничаване, спиране или отнемане на сертификат, сертифициращият орган трябва да отговаря на изискванията на раздел 7.11 ISO / IEC 17065:2012.

Сертифициращият орган информира в разумен срок Клиента и КЗЛД за причините за прекратяването, ограничаването, спирането или отнемането на сертификат в писмена форма.

Сертифициращият орган трябва да налага пропорционални и прогресивно отежнени санкции в случаите, в които Клиент е затаил, укрил или не е предоставил в срок информация, свързана с текущи производства или друга относима информация, свързана със спазването на изискванията на законодателството по защита на данните.

Сертифициращият орган е задължен да приема и прилага решенията и нарежданията на КЗЛД за отнемане или за не издаване сертификат на Клиент (Заявител), ако не са спазени или впоследствие (след получаване на сертификат) не се спазват изискванията за сертификация. Неприлагането на решенията на КЗЛД е самостоятелно основание за отнемане или не издаване/не подновяване на сертификат.

7.12 Записи

Сертифициращият орган трябва да съхранява записи в съответствие с точка 7.12 ISO / IEC 17065: 2012, за да докаже, че притежателят на сертификата отговаря на изискванията за сертифициране. Сертифициращия орган трябва да съхранява цялата документация в пълен, разбираем, актуален и подходящ за извършване на одит вид. На КЗЛД трябва да бъде предоставен достъп до тези записи по всяко време.

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

В допълнение на т. 7.13 ISO / IEC 17065: 2012, сертифициращият орган трябва да определи подходящи процедурни насоки за обработка на жалбите, които получава за нарушения или прилагане на изискванията за сертифициране от притежателите на сертификати, които включват и:

- определяне на лицата, които могат да подават жалби и сигнали;
- кой ще ги обработва от страна на Сертифициращият орган;
- какви са процедурите за проверката им;
- възможностите за връзка и събиране на информация от заинтересованите страни;
- как и на кого трябва да се даде подобно потвърждение;
- какви проверки могат да се проведат;
- кои процеси трябва да бъдат започнати след това;
- сроковете за проверка на жалбите.

Процедурните указания се публикуват по общодостъпен начин след акредитация на Сертифициращия орган.

Сертифициращият орган трябва да води регистър на жалбите, които е получил и предприетите мерки, както и трябва да предостави на КЗЛД достъп до това по всяко време.

В споразумението за сертифициране, в допълнение към изискванията по смисъла на точка 4.1.2 ISO / IEC 17065: 2012, трябва да се посочи задълженията на Сертифициращия орган във връзка с оплаквания относно спазването на изискванията за сертифициране, като по-специално създаване на вътрешен каталог от мерки за разглеждане на получените жалби и задължението за документиране и запазване на жалбите и предприетите мерки, както и за продължителността на съхранение, като се вземат предвид принципите за обработка на лични данни по смисъла на ОРЗД. Заявителят/Клиентът има задължение да информира в разумен срок Сертифициращият орган за потенциални причини за прекратяването, ограничаването, спирането или отнемането на сертификат.

В съответствие с т. 7.13 ISO / IEC 17065: 2012, сертифициращият орган трябва да определи подходящи процедурни насоки за обработка на жалбите, които получава за нарушения или прилагане на изискванията за сертифициране от притежателите на сертификати, като Сертифициращият орган трябва да определи процедури, гарантиращи 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 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 КЗЛД 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 срока на валидност на сертификатите, въз основа на каква рамка и при какви условия.

8.1 Общи изисквания към системата за управление

Прилагат се изискванията на ISO/IEC 17065/2012.

8.2 Документация на системата за управление

Прилагат се изискванията на ISO/IEC 17065/2012.

8.3 Контрол на документите

Прилагат се изискванията на ISO/IEC 17065/2012.

8.4 Контрол на записите

Прилагат се изискванията на ISO/IEC 17065/2012.

8.5 Преглед от ръководството

Прилагат се изискванията на ISO/IEC 17065/2012.

8.6 Вътрешни одити

Прилагат се изискванията на ISO/IEC 17065/2012.

8.7 Коригиращи действия

Прилагат се изискванията на ISO/IEC 17065/2012.

8.8 Предпазни действия

Прилагат се изискванията на ISO/IEC 17065/2012.

9 Други допълнителни изисквания

9.1 Актуализиране на методите за оценяване

Сертифициращият орган определя процедури по 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

Сертифициращият орган трябва да използва процедури, за да гарантира, че специализираните знания на персонала се актуализират, по-специално като се вземат предвид промените в правната ситуация, рискът за обработка и състоянието на техниката и технологиите.

9.3 Отговорности и компетенции

9.3.1 Комуникация между Сертифициращия орган и неговите клиенти

Сертифициращият орган трябва да разработи процедури за:

1. Поддържане на документация за:
- Отговори при искания за достъп до информация;
- Контактна точка, при разглеждането на жалби.
2. Процес по обработване на жалби:
   - информация за статуса на дадена жалба;
   - комуникация с и взимане предвид оценката на КЗЛД;

9.3.2 Документация на дейностите по оценяване

Не са предвидени допълнителни изисквания.

9.3.3 Управление на разглеждането на жалби

В съответствие с т. 7.13 ISO / IEC 17065: 2012, Сертифициращият орган трябва да определи подходящи процедурни насоки за обработка на жалбите, които получава за нарушения или прилагане на изискванията за сертифициране от притежателите на сертификати, като сертифициращият орган трябва да определи процедури, гарантиращи разделението между дейностите по сертифициране и обработката на оплаквания и жалби.

Сертифициращият орган трябва да води регистър на жалбите, които е получил и предприетите мерки, както и трябва да предостави на КЗЛД достъп до това по всяко време.

9.3.4 Управление на процедурата по оттегляне

В споразумението за сертифициране, в допълнение към изискванията по смисъла на точка 4.1.2 ISO / IEC 17065: 2012, трябва да се посочат задължения на кандидата за сертифициране във връзка с прекратяване, ограничаване, спиране или отнемане на сертифицирането.

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.

Сертифициращият орган информира КЗЛД за причините за прекратяването, ограничаването, спирането или отнемането на сертификат.