Насоки 1/2018 относно сертифицирането и определянето на критериите за сертифициране в съответствие с членове 42 и 43 от Регламента

Версия 3.0

4 юни 2019 г.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Приети

История на версиите

Версия 3.0	4 юни 2019 г.	Включване на приложение 2 (версия 2.0 на приложение 2, приета на 4 юни 2019 г. след обществена консултация)
Версия 2.1	9 април 2019 г.	Приемане на поправка на насоките (параграф 45)
Версия 2.0	23 януари 2019 г.	Приемане на насоките след обществена консултация — на същата дата беше прието приложение 2 (версия 1.0) за обществена консултация.
Версия 1.0	25 май 2018 г.	Приемане на насоките за обществена консултация

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 (наричан по-нататък „ОРЗД“),

като взе предвид Споразумението за ЕИП, и по-специално приложение XI и Протокол 37 от него, изменени с Решение № 154/2018 на Съвместния комитет на ЕИП от 6 юли 2018 г.,

като взе предвид членове 12 и 22 от своя Правилник за дейността от 25 май 2018 г.,

като отчете резултатите от обществената консултация относно насоките, проведена между 30 май 2018 г. и 12 юли 2018 г., и тази относно приложение 2, проведена между 15 февруари и 29 март 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) 2016/279, „ОРЗД“ или „Регламентът“) осигурява модернизирана рамка за отчетност и спазване на основните права по отношение на защитата на данните в Европа. Ключов елемент в тази нова рамка е въвеждането на набор от 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. Преди приемането на ОРЗД Работната група по член 29 установи, че сертифицирането би могло да изиграе важна роля при осигуряването на отчетност при защитата на данните[1]. За да се гарантира, че сертифицирането осигурява надеждни доказателства за спазването на изискванията за защита на данните, са необходими ясни правила, които да определят изискванията за сертифициране[2]. Член 42 от ОРЗД осигурява правното основание за разработването на такива правила.

3. В член 42, параграф 1 от ОРЗД се предвижда, че:

   „Държавите членки, надзорните органи, Комитетът по защита на данните и Комисията насърчават, особено на равнището на Съюза, създаването на механизми за сертифициране за защита на данните и на печати и маркировки за защита на данните с цел да се демонстрира спазването на настоящия регламент при операциите по

[1] Работна група по член 29, Становище 3/2010 относно принципа на отчетността, WP173, 13 юли 2010 г., точки 69—71.
[2] Работна група по член 29, Становище 3/2010 относно принципа на отчетността, WP173, точка 69.

обработване от страна на администраторите и обработващите лични данни. Отчитат се конкретните нужди на микропредприятията, на малките и средните предприятия.“

4. Механизмите за сертифициране3 могат да подобрят прозрачността както за субектите на данни, така и в отношенията между предприятията, например между администраторите и обработващите лични данни. 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 услуги4.

5. С ОРЗД не се въвежда право или задължение за сертифициране на администраторите и обработващите лични данни; според член 42, параграф 3 сертифицирането е доброволен процес, който спомага да се докаже спазването на ОРЗД. Държавите членки и надзорните органи се призовават да насърчават създаването на механизми за сертифициране и те ще определят участието на заинтересованите страни в процеса на сертифициране и неговия жизнен цикъл.

6. Освен това спазването на одобрените механизми за сертифициране е обстоятелство, което надзорните органи трябва да отчитат като утежняващ или смекчаващ фактор, когато вземат решение за налагане на административно наказание „глоба“ или „имуществена санкция“ и когато определят неговия размер (член 83, параграф 2, буква й))5.

1.1 Обхват на насоките

7. Настоящите насоки са ограничени по обхват; те не представляват наръчник с правила за сертифициране в съответствие с ОРЗД. Основната цел на настоящите насоки е да се определят най-общи изисквания и критерии, които може да бъдат подходящи за всички видове механизми за сертифициране, издавани в съответствие с членове 42 и 43 от ОРЗД. За тази цел насоките:

   - разглеждат основанието за сертифицирането като инструмент за отчетност;
   - разясняват ключовите понятия от разпоредбите за сертифициране по членове 42 и 43; и
   - разясняват обхвата на това, което може да се сертифицира по членове 42 и 43, както и целта на сертифицирането;

[3] В настоящите насоки механизмите за сертифициране и печатите и маркировките за защита на данните се наричат заедно „механизми за сертифициране“, вж. раздел 1.3.2.

[4] В съображение 100 се казва, че за да „се повишат прозрачността и съответствието с [настоящия] регламент, следва да се насърчава създаването на механизми за сертифициране [...], които позволяват на субектите на данни бързо да оценяват нивото на защита на данните на съответните продукти и услуги“.

[5] Вж. Работна група по член 29, Насоки относно прилагането и определянето на административните наказания „глоба“ или „имуществена санкция“ за целите на Регламент (ЕС) 2016/679 (WP 253).

- спомагат за постигането на съдържателен, недвусмислен, възпроизводим във възможно най-голяма степен и съпоставим резултат от сертифицирането, независимо от сертифициращия орган (съпоставимост).

8. ОРЗД допуска множество възможности за прилагане на членове 42 и 43 от страна на държавите членки и надзорните органи. Насоките дават съвети за тълкуването и изпълнението на разпоредбите на членове 42 и 43 и ще помогнат на държавите членки, надзорните органи и националните органи по акредитация да възприемат по-съгласуван и хармонизиран подход към прилагането на механизми за сертифициране в съответствие с ОРЗД.

9. Включените в насоките съвети ще бъдат от значение за:

   - компетентните надзорни органи и Европейския комитет по защита на данните („ЕКЗД“), когато одобряват критериите за сертифициране в съответствие с член 42, параграф 5, член 58, параграф 3, буква е) и член 70, параграф 1, буква о);
   - сертифициращите органи, когато изготвят и преразглеждат критериите за сертифициране, преди да ги представят на компетентния надзорен орган за одобрение съгласно член 42, параграф 5;
   - ЕКЗД, когато одобрява европейски печат за защита на данните в съответствие с член 42, параграф 5 и член 70, параграф 1, буква о);
   - надзорните органи, когато изготвят своите собствени критерии за сертифициране;
   - Европейската комисия, която е упълномощена да приема делегирани актове за определяне на изискванията, които следва да се вземат предвид за механизмите за сертифициране в съответствие с член 43, параграф 8;
   - ЕКЗД, когато предоставя на Европейската комисия становище относно изискванията за сертифициране в съответствие с член 70, параграф 1, буква р) и член 43, параграф 8;
   - националните органи по акредитация, които ще трябва да вземат предвид критериите за сертифициране с оглед на акредитирането на сертифициращите органи в съответствие с EN-ISO/IEC 17065/2012 и допълнителните изисквания в съответствие с член 43; и
   - администраторите и обработващите лични данни, когато определят своята собствена стратегия за спазване на ОРЗД и разглеждат сертифицирането като средство за доказване на спазването.

10. ЕКЗД ще публикува отделни насоки за определянето на критериите за одобряване на механизмите за сертифициране като инструменти за предаване на данни на трети държави или международни организации в съответствие с член 42, параграф 2.

1.2 Цел на сертифицирането по ОРЗД

11. В член 42, параграф 1 е предвидено, че механизмите за сертифициране следва да бъдат създадени „с цел да се демонстрира спазването на настоящия регламент при

операциите по обработване от страна на администраторите и обработващите лични данни“.

12. ОРЗД илюстрира контекста, в който одобрените механизми за сертифициране могат да бъдат използвани като елемент, който доказва, че администраторите и обработващите лични данни спазват задълженията си по отношение на:

    - прилагането и доказването на подходящи технически и организационни мерки съгласно посоченото в член 24, параграфи 1 и 3, член 25 и член 32, параграфи 1 и 3;
    - предоставянето на достатъчно гаранции съгласно член 28, параграф 5 (от обработващия лични данни на администратора), както е посочено в параграф 1 и (от подизпълнителя на обработващия лични данни) според параграф 4 от същия член.

13. Тъй като само по себе си сертифицирането не е доказателство за спазване на изискванията, а по-скоро е елемент, който може да се използва за доказване, то трябва да бъде извършвано по прозрачен начин. За доказване на спазването се изисква потвърждаваща документация, по-специално писмени доклади, които не само повтарят, но също така описват по какъв начин са изпълнени критериите, а ако първоначално не са били изпълнени, се описват корекциите и коригиращите действия, както и тяхната целесъобразност, като по този начин се дават мотивите за издаване или продължаване на сертификата. Това включва съдържанието на отделното решение за предоставяне, подновяване или оттегляне на даден сертификат. То трябва да представя основанията, аргументите и доказателствата, получени чрез прилагането на критериите, както и заключенията, решенията или изводите от фактите или предпоставките, събрани по време на сертифицирането.

1.3 Ключови понятия

14. В следващия раздел са разгледани ключовите понятия в членове 42 и 43. С този анализ се подобрява разбирането на основните термини и на обхвата на сертифицирането по ОРЗД.

1.3.1 Тълкуване на понятието „сертифициране“

15. ОРЗД не съдържа определение на понятието „сертифициране“. Международната организация по стандартизация (ISO) дава общо определение на сертифицирането като „предоставянето от независим орган на писмено уверение (сертификат), че въпросният продукт, услуга или система отговаря на специфични изисквания“. Сертифицирането е известно също така като „оценка за съответствие от трета страна“, а сертифициращите органи могат да бъдат наричани също „органи за оценка на съответствието“ (ООС). В стандарт EN-ISO/IEC 17000:2004 „Оценяване на съответствието — Речник и общи принципи“ (на който се позовава ISO17065) сертифицирането е определено като: „атестация от трета страна… за продукти, процеси и услуги“.

16. Атестацията е „издаване на документално потвърждение на база на взето решение след извършен преглед, с което се потвърждава, че изпълнението на специфични изисквания е доказано“ (раздел 5.2, ISO 17000:2004).

17. В контекста на сертифицирането по членове 42 и 43 от ОРЗД, сертифицирането трябва да се позовава на атестацията от трета страна относно операциите по обработване на данни от администратори и обработващи лични данни.

1.3.2 Механизми за сертифициране, печати и маркировки за защита на данните

18. ОРЗД не съдържа определение на „механизми за сертифициране, печати и маркировки“, като термините се използват заедно. Сертификатът представлява документално потвърждение за съответствие. За обозначаване на успешното изпълнение на сертификационната процедура може да се използва печат или маркировка за защита на данните. Печат или маркировка обикновено представлява лого или символ, чието наличие (в допълнение към сертификата) указва, че обектът на сертифицирането е бил подложен на независима оценка в процедура по сертифициране и отговаря на определените изисквания, посочени в нормативни документи, като наредби, стандарти или технически спецификации. Тези изисквания в контекста на сертифицирането по ОРЗД са определени в допълнителните изисквания, които допълват правилата за акредитиране на сертифициращите органи в EN-ISO/IEC 17065/2012, както и критериите за сертифициране, одобрени от компетентния надзорен орган или от Комитета. Сертификат, печат или маркировка според ОРЗД може да се издава само след независима оценка на доказателствата от акредитиран сертифициращ орган или компетентен надзорен орган, като се посочва, че критериите за сертифициране са изпълнени.

19. В таблицата е даден общ пример за процес на сертифициране.

Подаване на заявление от администратор или обработващ лични данни	Официална проверка от СО	Оценяване Предварителна оценка	Оценяване Оценка на ОнО	Оценяване Валидиране на резултатите	Информиране на компетентния надзорен орган	Сертифициране	Мониторинг	Подновяване на сертификат
Дали описанието на обекта на оценката (ОнО) е недвусмислено и ясно, включително интерфейсите? Може ли да се предостави достъп до дейностите по обработване на ОнО?	Може ли да бъде прието описанието на ОнО? Дали всички документи са интегрирани и актуални?	Кои са приложимите критерии? Кои са приложимите методи за оценка?	Отговаря ли ОнО на критериите? Вярна ли е документацията на ОнО?	Дали всички посочени релевантни критерии са приложени спрямо ОнО? Достатъчно добре ли е документирана оценката?	Посочени ли са мотивите за предоставяне или отнемане на сертификат?	Може ли да бъде предоставен сертификатът? Докладите [illegible] публикувани?	Дали ОнО продължава да отговаря на критериите? Правилно ли се използва сертификатът/ печатът/ маркировката?	Обработването все още ли отговаря на критериите за сертифициране? Дали е обърнато достатъчно внимание на аспекти, които могат да бъдат доразвити?
Член 42, параграф 6	Член 43, параграф 4	Член 43, параграф 4	Член 42, параграф 5, член 43, параграф 4	Член 43, параграф 4	Член 43, параграф 1, член 43, параграф 5	Член 43, параграф 1, член 42, параграф 7	Член 42, параграф 7	Член 42, параграф 7

2 РОЛЯТА НА НАДЗОРНИТЕ ОРГАНИ

20. В член 42, параграф 5 е предвидено, че сертификат се издава от акредитиран сертифициращ орган или от компетентен надзорен орган. Издаването на сертификати не е задължителна задача на надзорните органи съгласно ОРЗД. Напротив, ОРЗД допуска възможност за множество различни модели. Например надзорният орган може да избере един или повече от следните варианти:

    - да издава сертификати самостоятелно според своята собствена схема за сертифициране;
    - да издава сертификати самостоятелно според своята собствена схема за сертифициране, но да делегира на трети страни целия процес на оценяване или част от него;
    - да създаде своя собствена схема за сертифициране и да възложи процедурата по сертифициране на сертифициращи органи, които да издават сертификатите; и
    - да насърчава пазара да разработва механизми за сертифициране.

21. Надзорният орган ще трябва да разглежда своята роля, като вземе предвид и решенията, които са взети на национално ниво по отношение на механизмите за акредитация, по-специално ако самият надзорен орган е упълномощен да акредитира сертифициращи органи в съответствие с член 43, параграф 1 от ОРЗД. По този начин всеки надзорен орган ще определи кой подход да възприеме, за да изпълни широкото предназначение на сертифицирането по ОРЗД. Това ще бъде определено не само в зависимост от задачите и правомощията по членове 57 и 58, а също при отчитане на сертифицирането като фактор, който следва да се взема предвид при определяне на административните наказания „глоба“ или „имуществена санкция“, а в по-общ план, като средство за доказване на спазването на изискванията.

2.1 Надзорният орган като сертифициращ орган

22. Когато надзорният орган избере да извършва сертифициране, той ще трябва внимателно да прецени своята роля предвид възложените му задачи съгласно ОРЗД. Ролята му трябва да бъде прозрачна при упражняване на неговите функции. По-специално той ще трябва да обърне внимание на разделянето на правомощията, свързани с разследванията и правоприлагането, за да се избегнат потенциални конфликти на интереси.

23. Когато действа като сертифициращ орган, надзорният орган ще трябва да осигури надлежното създаване на механизъм за сертифициране и да разработи свои собствени критерии за сертифициране или да приеме такива. Освен това всеки надзорен орган, който издава сертификати, е натоварен със задачата да извършва периодичен преглед на тези сертификати (член 57, параграф 1, буква о)), както и с правомощието да ги

отнема, когато изискванията за сертифициране не са спазени или вече не се спазват (член 58, параграф 2, буква з)). За да бъдат изпълнени тези изисквания, е целесъобразно да се създаде процедура по сертифициране и да се изготвят изисквания по отношение на процеса, а когато не е предвидено друго, напр. в националното право, да се сключи правно обвързващо споразумение за извършване на дейностите по сертифициране с отделната кандидатстваща организация. Следва да се гарантира, че въз основа на това споразумение за сертифициране кандидатът е задължен да спазва най-малко критериите за сертифициране, в това число необходимите мерки за извършване на оценка, мониторинг на съответствието с критериите, както и периодичен преглед, включително достъп до информация и/или помещения, документация и публикуване на доклади и резултати, както и разследване на жалби. Освен това се очаква надзорният орган да спазва изискванията в насоките за акредитиране на сертифициращи органи в допълнение към изискванията по член 43, параграф 2.

2.2 Допълнителни задачи на надзорния орган по отношение на сертифицирането

24. В държави членки, в които започнат да действат сертифициращи органи, надзорният орган, независимо от своите собствени дейности, има правомощията и задачите:

    - да оценява критериите на схемата за сертифициране и да изготвя проект за решение (член 42, параграф 5);
    - да предава на Комитета проекта за решение, когато възнамерява да одобри критериите за сертифициране (член 64, параграф 1, буква в), член 64, параграф 7) и да взема предвид становището на Комитета (член 64, параграф 1, буква в) и член 70, параграф 1, буква у));
    - да одобри критериите за сертифициране (член 58, параграф 3, буква е)), преди да може да се извършва акредитиране и сертифициране (член 42, параграф 5 и член 43, параграф 2, буква б));
    - да публикува критериите за сертифициране (член 43, параграф 6);
    - да действа като компетентен орган за общоевропейски схеми за сертифициране, което може да доведе до одобрен от ЕКЗД „Европейски печат за защита на данните“ (член 42, параграф 5 и член 70, параграф 1, буква о)); и
    - да разпорежда на сертифициращ орган: а) да не издава сертификат или б) да отнеме сертификат, когато изискванията за сертифициране (процедури по или критерии за сертифициране) не са спазени или вече не се спазват (член 58, параграф 2, буква з).

25. Според ОРЗД надзорният орган е натоварен с одобряването на критерии за сертифициране, но не и с разработването на критерии. За да одобри критериите за сертифициране по член 42, параграф 5, надзорният орган трябва да има ясно разбиране

за това какво да очаква, по-специално във връзка с обхвата и съдържанието, за да се докаже спазване на ОРЗД, както и по отношение на своите задачи за мониторинг и осигуряване на прилагането на регламента. В приложението са дадени насоки за осигуряване на хармонизиран подход при оценяването на критерии за целите на одобряването.

26. Според член 43, параграф 1 се изисква сертифициращите органи да уведомяват техния надзорен орган, преди да издават или подновяват сертификати, за да може компетентният надзорен орган да упражни своите корективни правомощия по член 58, параграф 2, буква з). Освен това според член 43, параграф 5 сертифициращите органи са длъжни също така да представят на компетентния надзорен орган мотивите за издаване или отнемане на съответния сертификат. Въпреки че ОРЗД допуска надзорните органи да определят как да получават, потвърждават, преглеждат и третират тази информация в оперативен план (например това може да включва технологични решения, чрез които да се осъществява докладването на сертифициращите органи), могат да бъдат въведени процедура и критерии за обработване на информацията и докладите, които се представят от сертифициращия орган за всеки успешен проект на сертифициране в съответствие с член 43, параграф 1. Въз основа на тази информация надзорният орган може да упражнява своите правомощия, за да разпорежда на сертифициращия орган да отнеме или да не издаде даден сертификат (член 58, параграф 2, буква з)), както и да наблюдава и да осигурява прилагането на изискванията и критериите за сертифициране по ОРЗД (член 57, параграф 1, буква а) и член 58, параграф 2, буква з)). По този начин ще се осигури прилагането на хармонизиран подход и съпоставимост на сертифицирането от различни сертифициращи органи, а също така и информацията за статуса на сертификата на дадена организация ще бъде известна на надзорните органи.

3 РОЛЯ НА СЕРТИФИЦИРАЩИЯ ОРГАН

27. Ролята на сертифициращия орган е да издава, преглежда, подновява и отнема сертификати (член 42, параграфи 5 и 7) въз основа на механизъм за сертифициране и одобрени критерии (член 43, параграф 1). За тази цел сертифициращият орган или собственикът на схемата за сертифициране трябва да определи и установи критерии за сертифициране и процедури по сертифициране, включително процедури за мониторинг на спазването, преглед, обработване на жалби и отнемане. Критериите за сертифициране се преразглеждат като част от процеса на акредитация, в който се вземат предвид правилата и процедурите за издаване на сертификати, печати или маркировки (член 43, параграф 2, буква в)).

28. Сертифициращият орган трябва да има механизъм за сертифициране и критерии за сертифициране, за да получи акредитация по член 43. Дейностите на сертифициращия орган са повлияни до голяма степен от обхвата и вида на критериите за сертифициране, които влияят върху процедурите по сертифициране и обратно. Специфични критерии може например да предвиждат конкретни методи за оценяване, като инспекции на

място и преглед на кодекси. Тези процедури са задължителни за акредитирането и са разяснени допълнително в насоките за акредитиране.

29. В съответствие с ОРЗД сертифициращият орган е длъжен да предоставя на надзорните органи информация, особено по отделни сертификати, която е необходима да се наблюдава прилагането на механизма за сертифициране (член 42, параграф 7, член 43, параграф 5, член 58, параграф 2, буква з)).

4 ОДОБРЯВАНЕ НА КРИТЕРИИ ЗА СЕРТИФИЦИРАНЕ

30. Критериите за сертифициране представляват неразделна част от всеки механизъм за сертифициране. Затова според ОРЗД се изисква компетентният надзорен орган да одобри критериите за сертифициране на съответния механизъм за сертифициране (член 42, параграф 5 и член 43, параграф 2, буква б)). А когато се касае за Европейски печат за защита на данните, критериите за сертифициране се одобряват от ЕКЗД (член 42, параграф 5 и член 70, параграф 1, буква о)). По-долу са обяснени и двата варианта за одобряване на критерии за сертифициране.

31. ЕКЗД признава следните цели при одобряването на критерии за сертифициране:

- да отразяват надлежно установените в Регламент (ЕС) 2016/679 изисквания и принципи за защита на физическите лица във връзка с обработването на лични данни; и
- да допринасят за последователното прилагане на ОРЗД.

32. Одобрение се предоставя, ако критериите за сертифициране изцяло отразяват изискването на ОРЗД, че механизмът за сертифициране следва да позволява на администраторите и на обработващите лични данни да доказват спазването на ОРЗД.

4.1 Одобряване на критериите от компетентния надзорен орган

33. Критериите за сертифициране трябва да бъдат одобрени от компетентния надзорен орган преди или по време на процеса на акредитация на сертифициращия орган. Одобрение се изисква и за актуализирани или допълнителни схеми или набори от критерии по ISO 17065 на същия сертифициращ орган, преди използването им в изменените механизми за сертифициране (член 42, параграф 5 и член 43, параграф 2, буква б)). Надзорните органи трябва да третират всички искания за одобряване на критерии за сертифициране по справедлив и недискриминиращ начин, в съответствие с публично достъпна процедура, определяща общите условия, които трябва да бъдат изпълнени, и описанието на процеса на одобрение.

34. Сертифициращият орган може да издава сертификати само в определена държава членка в съответствие с критериите, които са одобрени от надзорния орган в тази държава членка. С други думи, критериите за сертифициране трябва да бъдат одобрени от компетентния надзорен орган, когато сертифициращият орган цели да предлага сертифициране и да получи акредитация. Вж. раздела по-долу относно общоевропейски схеми за сертифициране.

4.2 Одобряване на критерии от ЕКЗД за Европейски печат за защита на данните

35. Сертифициращият орган може също така да издава сертификати в съответствие с критерии, одобрени от ЕКЗД за Европейски печат за защита на данните. Критериите за сертифициране, одобрени от ЕКЗД по член 63, могат да доведат до Европейски печат за защита на данните (член 42, параграф 5). С оглед на съществуващите конвенции, касаещи аспектите на сертифициране и акредитация, ЕКЗД обръща внимание, че е желателно да се избягва фрагментиране на пазара на сертифицирането за защита на данните. Комитетът отбелязва, че в член 42, параграф 1 е предвидено, че държавите членки, надзорните органи, Комитетът и Комисията трябва да насърчават създаването на механизми за сертифициране, особено на равнището на Съюза.

4.2.1 Заявление за одобряване

36. Заявлението за одобряване на критерии от ЕКЗД по член 42, параграф 5 и член 70, параграф 1, буква о) трябва да се подава чрез компетентен надзорен орган и да съдържа намерението на собственика на схемата, кандидата или акредитирания сертифициращ орган да предлага критериите в рамките на механизъм за сертифициране, насочен към администратори и обработващи лични данни във всички държави членки. Когато компетентният надзорен орган счита, че критериите могат да бъдат одобрени от ЕКЗД, той предоставя проект за решение на ЕКЗД.

37. Изборът къде да бъде подадено заявлението за одобряване на критериите се извършва въз основа на мястото, където е разположено централното управление на собствениците на схемата за сертифициране или на сертифициращите органи.

38. Обикновено сертифициращият орган подава заявление в рамките на процеса на искане на акредитация или когато вече е акредитиран от компетентния надзорен орган или националния орган по акредитация в неговата държава членка. Когато сертифициращият орган вече е акредитиран за механизъм за сертифициране по ОРЗД, това може да улесни процеса на одобряване.

4.2.2 Критерии за Европейски печат за защита на данните

39. ЕКЗД координира процеса на оценяване и одобрява критериите за Европейски печат за защита на данните. Оценката обхваща области, като например обхвата на критериите и способността да служат за целите на единно сертифициране. Когато критериите са одобрени от ЕКЗД, от компетентния надзорен орган за мястото, където е централното управление на сертифициращия орган в ЕС, се очаква да обработва жалби относно самия механизъм и да информира другите надзорни органи. Този надзорен орган е компетентен също така да предприема мерки срещу сертифициращия орган. Съобразно обстоятелствата компетентният надзорен орган уведомява другите надзорни органи и ЕКЗД.

40. Критериите за сертифициране, предвидени за единно сертифициране, зависят от искания в общоевропейски мащаб и следва да предвиждат специален механизъм за отговор на тези искания. Европейските механизми за сертифициране трябва да са предвидени за употреба във всички държави членки. Въз основа на член 42, параграф 5 механизмът за Европейски печат за защита на данните, както и критериите по него, трябва да позволяват адаптиране, така че да бъдат отчитани националните разпоредби за конкретния сектор, когато е приложимо, например за обработването на данни в училищата, и да предвиждат прилагане в общоевропейски план.

41. Пример: Международно училище, предлагащо обучение на субекти на данни в Съюза, се намира в държава членка „А“. Училището желае да сертифицира своя процес на кандидатстване онлайн по общоевропейска схема за сертифициране, за да получи Европейски печат за защита на данните. Целта на това училище е на базата на Европейския печат за защита на данните да кандидатства за сертифициране на операциите по обработка, предлагано от сертифициращ орган, установен в държава членка „Б“. Критериите за получаване на печат, които са определени и документирани в съответния механизъм, трябва да са в състояние да отчитат приложимите в държава членка „А“ разпоредби за училищата. С критериите трябва да се изисква също така в рамките на процедурата на училището за кандидатстване онлайн да се предоставя информация и да се вземат предвид приложимите изисквания на държавата членка за защита на данните, които може да са различни от тези в други държави членки. Пример за това са наборът от лични данни, който се предоставя при кандидатстване, например оценки в детската градина или резултати от тестове, различните периоди на запазване, събирането или обработването на финансови или биометрични данни, ограниченията за по-нататъшното обработване.

- Критериите с високо ниво на важност за одобряване на механизъм за Европейски печат за защита на данните включват:
  - критерии, одобрени от Комитета,
  - прилагане в различните юрисдикции, като се отразяват, ако е целесъобразно, националните правни изисквания и специфичните за сектора разпоредби;
  -
- хармонизирани критерии, които могат да се адаптират, за да се отразят националните изисквания;
  - описание на механизма за сертифициране, в което се посочват;
  - споразуменията за сертифициране, признаващи общоевропейски изисквания,
  - процедури за осигуряване и предоставяне на решения при национални различия и за гарантиране, че печатът спомага да се докаже спазването на ОРЗД, и
  - езика на докладите, отнасящи се до всички засегнати надзорни органи.

42. Приложението също съдържа съвети относно критериите за Европейски печат за защита на данните.

4.2.3 Роля на акредитацията

43. Както е отбелязано в точка 4.2.1, когато се приеме, че критериите са подходящи за единно сертифициране, и те бъдат одобрени от Комитета като такива съгласно член 42, параграф 5, тогава сертифициращите органи могат да бъдат акредитирани да извършват сертифициране по тези критерии на равнището на Съюза.

44. Схеми, които са предназначени да се предлагат единствено в определени държави членки, не могат да кандидатстват за печати на ЕС. Акредитирането за Европейски печат за защита на данните налага акредитиране в държавата членка, в която се намира централното управление на сертифициращия орган, който възнамерява да прилага схемата, т.е. отговаря за издаването на сертификати и за управлението на дейностите по сертифициране на своите субекти и дъщерни структури в други държави членки. Когато други учреждения или звена управляват и изпълняват сертифициране самостоятелно, всяко такова учреждение или звено трябва да има отделна акредитация в държавата членка, в която е базирано. С други думи, акредитацията е необходима само в държавата членка, в която се намира централното управление на сертифициращия орган, когато единствено централното управление издава сертификати. Обратно, когато други учреждения на сертифициращия орган също издават сертификати, тези учреждения също трябва да бъдат акредитирани.

45. Следователно, ако сертифициращ орган не е бил акредитиран да извършва сертифициране според Европейския печат за защита на данните, тогава не може да се използват одобрените от ЕКЗД критерии и печатът не може да се предлага.

5 РАЗРАБОТВАНЕ НА КРИТЕРИИ ЗА СЕРТИФИЦИРАНЕ

46. Рамката за разработване на критерии за сертифициране е установена с ОРЗД. Макар че членове 42 и 43 уреждат основните изисквания по отношение на процедурата по сертифициране, като предвиждат и основните критерии за процедурите по сертифициране, базата на критериите за сертифициране трябва да произтича от принципите и правилата на ОРЗД и да допринася за получаването на увереност, че те са изпълнени.

47. Разработването на критерии за сертифициране трябва да се съсредоточава върху тяхната проверимост, значимост и уместност с цел да се докаже спазването на Регламента. Критериите за сертифициране трябва да бъдат формулирани така, че да са ясни и разбираеми и да позволяват практическото им прилагане.

48. Когато се изготвят критерии за сертифициране и ако е приложимо, трябва да се вземат предвид inter alia следните аспекти на спазването, които да подкрепят оценяването на операцията по обработване:

    - законосъобразността на обработването съгласно член 6;
    - принципите на обработването на данни съгласно член 5;
    - правата на субектите на данни съгласно членове 12—23;
    - задължението за уведомяване за нарушения на сигурността на данните съгласно член 33;
    - задължението за защита на данните на етапа на проектирането и по подразбиране съгласно член 25;
    - дали е била направена оценка на въздействието върху защитата на данните съгласно член 35, параграф 7, буква г), ако е приложимо; и
    - техническите и организационните мерки, които се прилагат съгласно член 32.

49. Степента, в която тези аспекти са отразени в критериите, може да е различна в зависимост от обхвата на сертифицирането, който може да включва вида на операцията(ите) по обработване и областта (напр. сектора на здравеопазването) на сертифицирането.

5.1 Какво може да се сертифицира по ОРЗД?

50. ЕКЗД счита, че ОРЗД предвижда широки граници на това какво може да се сертифицира по ОРЗД, стига акцентът да е поставен върху това да се оказва съдействие за демонстриране спазването на регламента при операциите по обработване от страна на администраторите и обработващите лични данни (член 42, параграф 1).

51. Когато се прави оценка на дадена операция по обработване, ако е приложимо, трябва да се вземат предвид следните три основни компонента:

    1. лични данни (материален обхват на ОРЗД);
    2. технически системи — инфраструктурата като хардуер и софтуер, използвана за обработването на личните данни; и
    3. процеси и процедури, свързани с операцията(ите) по обработване.

52. Всеки компонент, който се използва в операциите по обработване, трябва да подлежи на оценка спрямо определените критерии. Влияние може да окажат най-малко четири различни важни фактора: 1) организацията и правната структура на администратора или обработващия лични данни; 2) отделът, средата и хората, които участват в операцията(ите) по обработване; 3) техническото описание на елементите, които подлежат на оценка; и накрая 4) ИТ инфраструктурата, чрез която се извършва операцията по обработване, включително операционни системи, виртуални системи, бази данни, системи за автентификация и разрешаване, маршрутизатори и защитни

стени, системи за съхранение, комуникационна инфраструктура или интернет достъп и свързаните технически мерки.

53. И трите основни компонента са от значение за проектирането на процедури и критерии за сертифициране. Степента, в която се вземат предвид, може да варира в зависимост от обекта на сертифицирането. Например в някои случаи може някои компоненти да не се отчитат, ако се прецени, че не са от значение за обекта на сертифицирането.

54. ОРЗД съдържа допълнителни насоки, за да се уточни какво може да се сертифицира в съответствие с него. От член 42, параграф 7 следва, че сертификати в съответствие с ОРЗД се издават само на администраторите и обработващите лични данни, което изключва например сертифицирането на длъжностни лица по защита на данните. В член 43, параграф 1, буква б) се прави позоваване на ISO 17065, в който е уредена акредитацията на сертифициращи органи, които оценяват съответствието на продукти, услуги и процеси. Дадена операция или набор от операции по обработване може да доведе до продукт или услуга според терминологията на ISO 17065 и съответно може да подлежи на сертифициране. Например обработването на данни на служителите с цел изплащане на заплатите или управление на отпуските представлява набор от операции по смисъла на ОРЗД и може да доведе до продукт, процес или услуга според терминологията на ISO.

55. Въз основа на тези съображения ЕКЗД счита, че обхватът на сертифицирането по ОРЗД е насочен към операции или набори от операции по обработване. Може да става въпрос за управленски процеси, т.е. организационни мерки, които следователно са неразделна част от операцията по обработване (напр. управленски процес, създаден за обработването на жалби в рамките на обработването на данни на служителите с цел изплащане на заплатите).

56. За да се оцени съответствието на операцията по обработване с критериите за сертифициране, трябва да се даде пример за използване. Например съответствието на използването на техническа инфраструктура в рамките на операция по обработване зависи от категориите данни, които тя е предназначена да обработва. Организационните мерки зависят от категориите и обема на данните и от техническата инфраструктура, използвана за обработването, като се вземат предвид характерът, обхватът, съдържанието и целите на обработването, както и рисковете за правата и свободите на субектите на данни.

57. Освен това трябва да се има предвид, че ИТ приложенията могат да варират в широки граници, макар да обслужват едни и същи цели на обработването. Следователно това може да се вземе предвид при определянето на приложното поле на механизмите за сертифициране и при изготвянето на критериите за сертифициране, т.е. обхватът на сертифицирането и критериите не трябва да бъдат твърде тесни, че да изключват ИТ приложения, проектирани по различен начин.

5.2 Определяне на обекта на сертифицирането

58. Трябва да се прави разлика между обхвата на механизма за сертифициране и неговия обект — наричан също обект на оценката (ОнО) — в рамките на отделните проекти за

сертифициране по даден механизъм за сертифициране. Обхватът на механизма за сертифициране може да бъде определен или в общ план, или по отношение на конкретен вид или област на операции по обработване и съответно може вече да посочва обектите на сертифициране, които попадат в обхвата на механизма за сертифициране (напр. сигурно съхранение и защита на личните данни, съдържащи се в дадено цифрово хранилище). Във всеки случай надлежна, съдържателна оценка на съответствието може да се направи само ако отделният обект на проекта за сертифициране е описан с точност. Трябва ясно да се опише кои операции по обработване са включени в обекта на сертифицирането и след това основните компоненти, т.е. кои данни, процеси и техническа инфраструктура ще се оценяват и кои не. В тази връзка винаги трябва да се вземат предвид и да се описват също така интерфейсите с други процеси. Ясно е, че в оценката не могат да се включат аспекти, които не са известни и съответно не могат да бъдат сертифицирани. Във всеки случай отделният обект на сертифициране трябва да има логична връзка с посланието или твърдението,отправяно със сертифицирането, и не трябва да заблуждава ползвателя, клиента или потребителя.

59. [Пример 1]

Банка предлага на своите клиенти уебсайт за онлайн банкиране. В рамките на тази услуга има възможност за извършване на преводи, купуване на акции, иницииране на периодични преводи и управление на сметка. Банката желае да сертифицира следните задачи по механизъм за сертифициране на защитата на данните с общ обхват въз основа на общи критерии:

а) сигурно влизане в услугата

Сигурното влизане е операция по обработване, която е разбираема за крайния ползвател и която е от значение от гледна точка на защитата на данни, тъй като изпълнява важна роля за гарантиране на сигурността на използваните лични данни. Затова тази операция по обработване е необходима за сигурното влизане и съответно може да представлява логичен обект на оценка (ОнО), ако в сертификата ясно е посочено, че единствено операцията по обработване за влизане е сертифицирана.

б) потребителски интерфейс (Web front-end)

Макар че потребителският интерфейс може да е от значение от гледна точка на защитата на данните, той не е разбираем за крайния ползвател и следователно не може да бъде логичен ОнО. Освен това за ползвателя не е ясно кои услуги на уебсайта и съответно кои операции по обработване са обхванати от сертифицирането.

в) онлайн банкиране

Потребителският интерфейс и сървърната част (back-end) са операции по обработване, които се предоставят в рамките на услугата за онлайн банкиране и които могат да имат смисъл за ползвателя. В този контекст и двата елемента трябва да бъдат включени в ОнО. Макар че операциите по обработване, които не са пряко свързани с предоставянето на услугата за онлайн банкиране, като

операции по обработването за целите на предотвратяване на изпирането на пари, може да бъдат изключени от ОнО.

Услугите за онлайн банкиране обаче, които банката предлага чрез своя уебсайт, могат да включват и други услуги, които от своя страна изискват техни собствени операции по обработка. В този контекст другите услуги могат да включват например предлагането на застрахователен продукт. Тъй като тази допълнителна услуга не е пряко свързана с целта да се предоставят услуги за онлайн банкиране, тя може да бъде изключена от ОнО. Ако тази допълнителна услуга (застраховка) бъде изключена от ОнО, интерфейсите за тази услуга, които са интегрирани на уебсайта, са част от ОнО и поради това трябва да бъдат описани, за да се прави ясно разграничение между услугите. Това описание е необходимо, за да се идентифицират и оценят възможните потоци от данни между двете услуги.

60. [Пример 2]

Банка предлага на своите клиенти услуга, която им дава възможност да съберат на едно място информацията, свързана с различни сметки и кредитни карти от няколко банки (събиране на едно място на информацията от банкови сметки). Банката желае услугата ѝ да бъде сертифицирана по ОРЗД. Компетентният надзорен орган е одобрил специален набор от критерии за сертифициране, съсредоточен върху този тип дейност. Обхватът на механизма за сертифициране е насочен само към следните аспекти на съответствието:

- автентификация на потребителя; и
- приемливи начини за получаване на данните, които следва да бъдат събрани на едно място от други банки/услуги.

Тъй като със самия обхват на този механизъм за сертифициране се определя ОнО, не е възможно ОнО да се стесни по смислен начин съгласно предложения обхват и да се сертифицират само конкретни характеристики или отделна дейност по обработване. При този сценарий ОнО трябва да бъде идентичен с конкретния обхват.

5.3 Методи за оценка и методика на оценяването

61. За оценката на съответствието, която спомага да се докаже съответствието на операциите по обработване, е необходимо да се набележат и определят методите за оценка и методиката на оценяването. Има значение дали информацията за оценяването е събрана само от документация (което само по себе си не би било достатъчно) или дали е събирана активно на място и чрез пряк или непряк достъп. Начинът, по който е събрана информацията, оказва въздействие върху значимостта на сертифицирането и поради това следва да бъде определен и описан.

Процедурите за издаване и периодичен преглед на сертификати следва да включват спецификации, за да се определи подходящото ниво на оценката (задълбоченост и детайлност), за да бъдат изпълнени критериите за сертифициране, както и да включват предоставянето на:

- информация и спецификации за прилаганите методи за оценка и събраните констатации, например от одити на място или от документация;
- методи за оценка, съсредоточени върху операциите по обработване (данни, системи, процеси) и целта на обработването;
- определяне на категориите данни, нуждите от защита и дали участват обработващи лични данни или трети страни;
- определяне на ролите и наличие на механизъм за контрол на достъпа, изграден въз основа на роли и отговорности.

62. Задълбочеността на оценката оказва въздействие върху значимостта и стойността на сертифицирането. Колкото по-малко задълбочена е оценката поради прагматични съображения или с цел да се понижат разходите, толкова по-ниска ще бъде и значимостта на сертифицирането на защитата на данните. От друга страна, решенията доколко детайлна да бъде оценката, може да надвишат финансовите възможности на заявителя, а често и възможностите на оценителите и одиторите. За да се докаже съответствие с правилата, невинаги е от решаващо значение анализът на използваните ИТ системи да бъде много подробен, за да бъде от значение.

5.1 Документиране на оценката

63. Сертифицирането трябва да се документира изчерпателно и всеобхватно. Ако няма документация, не може да се направи надлежна оценка. Основната функция на документирането на сертифицирането е да осигури прозрачност в процеса на оценяване в рамките на механизма за сертифициране. Документирането дава отговори на въпроси относно изискванията, които са определени по закон. В механизмите за сертифициране трябва да се предвиди стандартизирана методика за документиране. След това оценката ще позволява съпоставяне на документацията на сертифицирането с реалното състояние на място и спрямо критериите за сертифициране.

64. Всеобхватното документиране на онова, което е било сертифицирано, и на използваната методика спомага за постигането на прозрачност. В съответствие с член 43, параграф 2, буква в) с механизмите за сертифициране трябва да бъдат установени процедури, позволяващи прегледа на сертификатите. За да може надзорният орган да прецени дали и до каква степен сертифицирането може да се потвърди в официални разследвания, подробното документиране може да е най-подходящото средство за осведомяване. Затова документирането, което се прави в хода на оценката, трябва да бъде съсредоточено върху три основни аспекта:
    - съгласуваност и последователност на приложените методи за оценка;
    - методи за оценка, насочени към доказване на съответствието на обекта на сертифициране с критериите за сертифициране и съответно с Регламента; и
    - че резултатите от оценката са били валидирани от независим и безпристрастен сертифициращ орган.

5.5 Документиране на резултатите

65. В съображение 100 е дадена информация относно целите, които се преследват с въвеждането на сертифициране.

„За да се повишат прозрачността и съответствието с настоящия регламент, следва да се насърчава създаването на механизми за сертифициране, както и на печати и маркировки за защита на данните, които позволяват на субектите на данни бързо да оценяват нивото на защита на данните на съответните продукти и услуги.“

66. Документирането и съобщаването на резултатите изпълняват важна роля за повишаването на прозрачността. Сертифициращите органи, които използват механизми за сертифициране, печати или маркировки, насочени към субектите на данни (в качеството им на потребители или клиенти) трябва да осигурят лесно достъпна, разбираема и съдържателна информация относно сертифицираната(ите) операция(и) по обработване. Тази публична информация следва да включва най-малко:

- описание на ОнО;
- препратка към одобрените критерии, приложени за конкретния ОнО;
- методиката за оценяване на критериите (оценка на място, документиране и т.н.); и
- продължителността на валидност на сертификата; и
- да дава възможност на надзорните органи и обществеността за съпоставяне на резултатите.

6 НАСОКИ ЗА ОПРЕДЕЛЯНЕТО НА КРИТЕРИИ ЗА СЕРТИФИЦИРАНЕ

67. Критериите за сертифициране са неразделна част от механизма за сертифициране. Процедурата за сертифициране включва изискванията за това как, от кого, до каква степен и детайлността на оценката, която трябва да се направи в отделни проекти за сертифициране по отношение на определен обект на оценката (ОнО). Критериите за сертифициране съдържат номиналните изисквания, спрямо които се оценява реалната операция по обработване, определена в ОнО. Настоящите насоки за определяне на критериите за сертифициране съдържат общи съвети, които ще улеснят оценяването на критериите за сертифициране за целите на одобрението.

- Когато се одобряват или определят критерии за сертифициране, трябва да се вземат предвид следните общи съображения. Критериите за сертифициране трябва:
- да бъдат единни и проверими;

- да позволяват извършването на одит, за да се улесни оценката на операциите по обработване в съответствие с ОРЗД, като се посочат по-специално целите и насоките за постигането на тези цели;
- да бъдат от значение за целевата аудитория (напр. отношения между предприятия (B2B) и между предприятия и клиенти (B2C);
- да вземат предвид и ако е целесъобразно, да бъдат оперативно съвместими с други стандарти (като стандарти ISO, стандарти на национално ниво); и
- да бъдат гъвкави и приложими в различен мащаб, за да могат да се прилагат към различни по вид и размер организации, в това число микро, малки и средни предприятия в съответствие с член 42, параграф 1, и към основания на риска подход в съответствие със съображение 77.

68. Малко местно дружество, напр. търговец на дребно, обикновено осъществява по-прости операции по обработване, отколкото голям многонационален търговец на дребно. Макар че изискванията за законосъобразост на операциите по обработване са едни и същи, трябва да се вземат предвид обхватът на обработването на данни и неговата сложност; от това следва, че е необходимо механизмите за сертифициране и техните критерии да могат да се прилагат в различен мащаб според съответната дейност по обработване.

6.1 Съществуващи стандарти

69. Сертифициращите органи ще трябва да разгледат по какъв начин в конкретните критерии са взети предвид съществуващите съответни инструменти като кодекси на поведение, технически стандарти или национални регулаторни и правни инициативи. В идеалния случай критериите ще бъдат оперативно съвместими със съществуващите стандарти, което може да помогне на администратора или обработващия лични данни да изпълнят своите задължения по ОРЗД. Често обаче секторните стандарти са съсредоточени върху защитата срещу заплахи и сигурността на организацията, докато ОРЗД е насочен към защитата на основните права на физическите лица. Тази различна перспектива трябва да се вземе предвид, когато се проектират критерии или се одобряват критерии или механизми за сертифициране въз основа на секторни стандарти.

6.2 Определяне на критерии

70. Критериите за сертифициране трябва да съответстват на заявлението за сертифициране (послание или твърдение) на даден механизъм или схема за сертифициране и да отговарят на очакванията, които пораждат. Наименованието на механизма за сертифициране може вече да определя приложното поле и ще има последици за определянето на критерии.

71. [Пример 3]

Обхватът на механизъм, наречен „HealthPrivacyMark“, следва да се ограничи до сектора на здравеопазването. Наименованието на печата поражда очакването, че изискванията за защита на данните са били проверени във връзка със здравните данни. Съответно критериите на този механизъм трябва да са подходящи за оценяване на изискванията за защита на данните в този сектор.

72. [Пример 4]

    Механизъм, свързан със сертифицирането на операции по обработване, които включват системи за управление при обработването на данни, трябва да определи критерии, позволяващи признаването и оценяването на процесите на управление, както и съпътстващите ги технически и организационни мерки.

73. [Пример 5]

    Критериите за механизъм, свързан с изчисления в облак, трябва да отчитат специалните технически изисквания, необходими за използването на услуги в облак. Например ако се използват сървъри извън ЕС, в критериите трябва да се вземат предвид условията, определени в глава V от ОРЗД по отношение на предаването на данни към трети държави.

74. Критериите, които са проектирани да обслужват различни ОнО в различни сектори и/или държави членки, трябва да позволяват да бъдат прилагани при различни сценарии; да позволяват определянето на подходящи мерки, които съответстват на различни по размер операции по обработване (малки, средни или мащабни) и отразяват рискове с различна вероятност и сериозност за правата и свободите на физическите лица в съответствие с ОРЗД. Следователно процедурите за сертифициране (напр. за документиране, изпитване или метод за извършване на оценка и задълбоченост на тази оценка), които допълват критериите, трябва да отговарят на тези нужди и да допускат и съдържат правила, например за прилагането на съответните критерии в индивидуални проекти за сертифициране. Критериите трябва да улесняват оценката на това дали са предоставени достатъчни гаранции за изпълнението на подходящи технически и организационни мерки.

6.3 Продължителност на действие на критериите за сертифициране

75. Въпреки че критериите за сертифициране трябва да останат надеждни с течение на времето, те не следва да се разглеждат като постоянна величина. Те трябва да подлежат на преглед, например когато:

    - правната рамка е изменена;
    - има тълкуване на дадени условия и разпоредби в решения на Съда на Европейския съюз; или
    - са реализирани нови технически постижения.

За Европейския комитет по защита на данните,

Председател

(Андреа Йелинек)

ПРИЛОЖЕНИЕ 1: ЗАДАЧИ И ПРАВОМОЩИЯ НА НАДЗОРНИТЕ ОРГАНИ ПО ОТНОШЕНИЕ НА СЕРТИФИЦИРАНЕТО В СЪОТВЕТСТВИЕ С ОРЗД

	Разпоредби	Изисквания
Задачи	Член 43, параграф 6	От надзорния орган се изисква да оповести критериите, посочени в член 42, параграф 5, в леснодостъпна форма и да ги предаде на Комитета.
	Член 57, параграф 1, буква н)	От надзорния орган се изисква да одобри критериите за сертифициране съгласно член 42, параграф 5.
	Член 57, параграф 1, буква о)	Предвидено е, че, когато е приложимо (т.е. когато издава сертификат), той следва да извършва периодичен преглед на сертификатите, издадени в съответствие с член 42, параграф 7.
	Член 64, параграф 1, буква в)	От надзорния орган се изисква да предава проекта на решение на Комитета, когато целта е одобряване на критериите за сертифициране, посочени в член 42, параграф 5.
Правомощия	Член 58, параграф 1, буква в)	Предвидено е, че надзорният орган има правомощия да извършва преглед на сертификатите, издадени в съответствие с член 42, параграф 7.
	Член 58, параграф 2, буква з)	Предвидено е, че надзорният орган има правомощия да отнема сертификат или да разпореди на сертифициращия орган да отнеме сертификат, или да разпореди на сертифициращия орган да не издава сертификат.
	Член 58, параграф 3, буква д)	Предвидено е, че надзорният орган има правомощия да акредитира сертифициращи органи.
	Член 58, параграф 3, буква е)	Предвидено е, че надзорният орган има правомощия да издава сертификати и да одобрява критерии за сертифициране.
	Член 58, параграф 3, буква д)	Предвидено е, че надзорният орган има правомощия да акредитира сертифициращи органи.
	Член 58, параграф 3, буква е)	Предвидено е, че надзорният орган има правомощия да издава сертификати и да одобрява критерии за сертифициране.

ПРИЛОЖЕНИЕ 2:

1 ВЪВЕДЕНИЕ

Приложение 2 съдържа насоки за преглед и оценка на критериите за сертифициране съгласно член 42, параграф 5. В него се определят теми, които надзорният орган по защита на данните и Европейският комитет по защита на данните ще разглеждат и ще прилагат при одобряването на критерии за сертифициране на механизъм за сертифициране. Сертифициращите органи и собствениците на схеми, които желаят да изготвят и представят критерии за одобрение, следва да разгледат въпросите. Списъкът не е изчерпателен, но представя минималния брой теми, които да бъдат разгледани. Не всички въпроси ще бъдат приложими; те обаче следва да бъдат взети предвид при изготвянето на критериите и може да се наложи да се даде обяснение защо критериите не обхващат конкретни аспекти. Някои въпроси се повтарят, тъй като се поставят от различни гледни точки. Тези насоки следва да се разглеждат в съответствие с правните изисквания, предвидени от ОРЗД, и когато е приложимо, от националното законодателство.

2 ОБХВАТ НА МЕХАНИЗМА ЗА СЕРТИФИЦИРАНЕ И ОБЕКТ НА ОЦЕНКАТА (ОНО)

а. Ясно ли е описан обхватът на механизма за сертифициране (за който ще се използват критериите за защита на данните)?

б. Дали обхватът на механизма за сертифициране е съдържателен за аудиторията, за която е предназначен, и не е подвеждащ?

- *Пример: Печатът „ползващо се с доверие дружество“ предполага, че са били одитирани дейностите по обработка на данни на цялото дружество, въпреки че в действителност само определени операции по обработване, например процедурата за онлайн плащане, са обект на сертифициране. Следователно обхватът е подвеждащ.*

в. Дали обхватът на механизма за сертифициране отразява всички съответни аспекти на операциите по обработване?

- *Пример: Маркировката „Защита на неприкосновеността на личния живот в областта на здравето“ трябва да включва всички данни от оценката, отнасящи се до здравето, с цел да се отговори на изискванията по член 9.*

г. Позволява ли обхватът на механизма за сертифициране извършването на съдържателно сертифициране за защита на данните, като се вземат предвид естеството, съдържанието, рискът от свързаните операции по обработване на данни?

- *Пример: Ако обхватът на механизма за сертифициране е насочен само към специфични аспекти на операциите по обработване, като например събирането на данни, но не и върху други операции по обработване, като обработване с цел създаване на рекламни профили или управление на правата на субектите на данни, той няма да бъде съдържателен за субектите на данни.*

д. Дали обхватът на механизма за сертифициране включва обработването на лични данни в съответната държава, в която е подадено заявлението, или се отнася до презграничното обработване и/или предаване?

е. Критериите за сертифициране описват ли в достатъчна степен по какъв начин трябва да бъде дефиниран обектът на оценката?

- *Пример: „Печат за неприкосновеност на личния живот“, който предлага общ обхват, изискващ само „посочване на обработването, което подлежи на сертифициране“, не предоставя достатъчно ясни насоки за това как да се определя и описва обектът на оценката.*
- *Пример: Обхватът (или специфичният обхват) на „Марка за хранилище за неприкосновеност на личния живот“, която се отнася до сигурно съхранение, следва подробно да опише изискванията за постигане на този обхват в своите критерии, например определение на хранилище, системни изисквания, задължителни технически и организационни мерки. В този случай обхватът може ясно да даде определение на ОнО.*

(1) Изискват ли критериите ОнО да включва определяне на всички релевантни операции по обработване, онагледяване на потоците от данни и определяне на областта на прилагане на ОнО?

- *Пример: Механизъм за сертифициране предлага сертифициране на операциите по обработване на данни от администраторите съгласно ОРЗД, без допълнително да уточнява областта на прилагане (общ обхват). Критериите, използвани от механизма, изискват от кандидатстващия администратор да определи целевата операция по обработване (ОнО) по отношение на видовете данни, използваните системи и процеси.*

(2) Критериите изискват ли от заявителя ясно да укаже къде започва и къде приключва обработването, което е предмет на оценка? Критериите изискват ли ОнО да включва интерфейсите, в които взаимозависими операции по обработване не са включени като част от ОнО? Дадено ли е задоволително обоснование за това?

- *Пример: ОнО, който описва подробно функционирането по отношение на обработката на интернет услуга, включително регистрация на ползвателите, предоставяне на услугата, фактуриране, регистриране на IP адреси, връзки с ползватели и трети страни и с изключение на хостване на сървъра (но включително споразумения за обработване и технически и организационни мерки).*

ж. Критериите гарантират ли, че (индивидуалните) ОнО са разбираеми за аудиторията, включително субектите на данни, когато е уместно?

3 ОБЩИ ИЗИСКВАНИЯ

а. Дали всички релевантни термини, използвани в каталога от критерии (т.е. всички критерии за сертифициране), са ясно определени, обяснени и описани?

б. Определени ли са всички нормативни препратки?

в. Критериите включват ли определяне на свързаните със защита на данните отговорности, процедури и обработване, обхванати от обхвата на механизма за сертифициране?

4 ОПЕРАЦИИ ПО ОБРАБОТВАНЕ, ЧЛЕН 42, ПАРАГРАФ 1

По отношение на обхвата на механизма за сертифициране (общ или специфичен) критериите разглеждат ли всички съответни елементи на операциите по обработване (данни, системи и процеси)?

а. Критериите изискват ли определяне на валидните правни основания за обработване по отношение на ОнО?

б. По отношение на ОнО критериите отчитат ли съответните фази на обработване и целия жизнен цикъл на данните, включително заличаване и/или анонимизиране?

в. По отношение на ОнО критериите изискват ли преносимост на данните?

г. По отношение на ОнО критериите позволяват ли да бъдат установени и отразени специални видове операции по обработване, например за автоматизирано вземане на решения, профилиране?

д. По отношение на ОнО критериите позволяват ли установяването на специални категории данни?

е. Критериите позволяват ли и изискват ли извършването на оценка на риска на отделните операции по обработване и оценка на необходимостта от защита за правата и свободите на субектите на данни?

ж. Критериите позволяват ли и изискват ли подходящо отчитане на рисковете за правата и свободите на физическите лица?

...

5 ЗАКОНОСЪОБРАЗНОСТ НА ОБРАБОТВАНЕТО

а. Критериите изискват ли проверка на законосъобразността на обработването за отделните операции по обработване по отношение на целта и необходимостта от обработване?

б. Критериите изискват ли да се извърши проверка на всички изисквания на правното основание за отделните операции по обработване?

6 ПРИНЦИПИ, ЧЛЕН 5

а. Критериите разглеждат ли по подходящ начин всички принципи за защита на данните в съответствие с член 5?

б. Критериите изискват ли доказателства за свеждане до минимум на данните за всеки отделен ОнО?

...

7 ОБЩИ ЗАДЪЛЖЕНИЯ НА АДМИНИСТРАТОРИТЕ И ОБРАБОТВАЩИТЕ ЛИЧНИ ДАННИ

а. Критериите изискват ли доказателства за договорни споразумения между обработващите лични данни и администраторите?

б. Споразуменията между обработващите лични данни и администраторите подлежат ли на оценка?

в. Критериите отразяват ли задълженията на администратора съгласно глава IV?

г. Критериите изискват ли доказателства за преглед и актуализация на техническите и организационните мерки, приложени от администратора съгласно член 24, параграф 1?

д. Критериите проверяват ли дали организацията е направила оценка на необходимостта от назначаване на длъжностно лице за защита на данните (ДЗД) съгласно изискванията на член 37? Когато това е целесъобразно, ДЗД отговаря ли на изискванията по членове 37—39?

е. Критериите проверяват ли дали се изискват регистри на дейностите по обработване съгласно член 30, параграф 5 и отговарят ли по подходящ начин на изискванията на член 30?

8 ПРАВА НА СУБЕКТИТЕ НА ДАННИ

а. Критериите включват ли по подходящ начин правото на информация на субекта на данни и изискват ли да бъдат въведени съответни мерки?

б. Критериите изискват ли подходящ или по-голям достъп и контрол на субектите на данни по отношение на техните данни, включително преносимост на данните?

в. Критериите изискват ли въвеждането на мерки, които предвиждат възможност за намеса в операцията по обработване, с цел да се гарантират правата на субектите на данни и да се позволи извършването на корекции, заличаване или ограничаване?

...

9 РИСКОВЕ ЗА ПРАВАТА И СВОБОДИТЕ НА ФИЗИЧЕСКИТЕ ЛИЦА

а. Критериите позволяват ли и изискват ли извършването на оценка на риска за правата и свободите на физическите лица?

б. Критериите предвиждат ли или изискват ли използването на призната методология за оценка на риска? Ако е уместно, това пропорционално ли е?

в. Критериите позволяват ли и изискват ли извършването на оценка на въздействието на предвидените операции по обработване върху правата и свободите на физическите лица?

г. Критериите изискват ли предварителна консултация относно оставащите рискове, които не могат да бъдат смекчени, въз основа на резултатите от оценката на въздействието върху защитата на данните (ОВЗД)?

10 ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ, ГАРАНТИРАЩИ ЗАЩИТА

а. Критериите изискват ли прилагането на технически и организационни мерки, предвиждащи поверителност на операциите по обработване?

б. Критериите изискват ли прилагането на технически и организационни мерки, предвиждащи цялостност на операциите по обработване?

в. Критериите изискват ли прилагането на технически и организационни мерки, предвиждащи наличност на операциите по обработване?

г. Критериите изискват ли прилагането на мерки, които предвиждат прозрачност на операциите по обработка по отношение на:

д. отчетността?

е. правата на субектите на данни?

ж. оценката на отделните операции по обработване, например прозрачност на алгоритмите?

з. Критериите изискват ли прилагането на технически и организационни мерки, които гарантират правата на субектите на данни, например способността за предоставяне на информация или за преносимост на данните?

и. Критериите изискват ли прилагането на технически и организационни мерки, които предвиждат възможност за намеса в операцията по обработване, с цел да се гарантира правото на субектите на данни и да се позволи извършването на корекции, заличаване или ограничаване?

й. Критериите изискват ли прилагането на мерки, които предвиждат възможност за намеса в операцията по обработване с цел коригиране или проверка на системата или процес?

к. Критериите изискват ли прилагането на технически и организационни мерки, за да се гарантира свеждане на данните до минимум, например несвързване или отделяне на данните от субекта на данните, анонимизиране или псевдонимизиране, или изолиране на системите за данни?

л. Критериите изискват ли технически мерки за прилагане на защита на данните по подразбиране?

м. Критериите изискват ли технически и организационни мерки за прилагане на защитата на данните още при проектирането, например система за управление на защитата на данните, която да демонстрира, формира, контролира и прилага изискванията за защита на данните?

н. Критериите изискват ли технически и организационни мерки за изпълнение на подходящо периодично обучение и образование за персонала, който има постоянен или редовен достъп до лични данни?

о. Критериите изискват ли мерки за преразглеждане?

п. Критериите изискват ли самооценка/вътрешен одит?

р. Критериите изискват ли мерки, за да се гарантира, че задълженията за уведомяване при нарушение на сигурността на личните данни се изпълняват своевременно и с подходящ обхват?

с. Критериите изискват ли въвеждането и проверката на процедури за управление на инциденти?

т. Критериите изискват ли проследяване на развитието на въпросите, свързани с неприкосновеността на личния живот и технологиите, и актуализиране на схемата според необходимото?

...

11 ДРУГИ СПЕЦИФИЧНИ ХАРАКТЕРИСТИКИ, БЛАГОПРИЯТСТВАЩИ ЗАЩИТАТА НА ДАННИТЕ

а. Критериите изискват ли прилагането на техники за подобряване на защитата на данните? Това може да включва критерии, които изискват засилена защита на данните чрез премахване или намаляване на личните данни и/или на риска във връзка със защитата на данните.

- *Пример: Критерии, които изискват по-голямо намаляване на възможността за намиране на връзка чрез използването на ориентирано към потребителя управление на самоличността, като например проверка на самоличността, основана на атрибутите (attribute –based credentials - ABC), вместо ориентирано към организацията управление на самоличността, биха били отражение на техника за подобряване на защитата на данните.*

б. Критериите изискват ли прилагането на по-голям контрол от страна на субектите на данни, за да се улеснят самоопределението и изборът?

...

12 КРИТЕРИИ ЗА ДОКАЗВАНЕ НАЛИЧИЕТО НА ПОДХОДЯЩИ ГАРАНЦИИ ЗА ПРЕДАВАНЕТО НА ЛИЧНИ ДАННИ

Критериите ще бъдат разгледани в предстоящи насоки по член 42, параграф 2.

13 ДОПЪЛНИТЕЛНИ КРИТЕРИИ ЗА ЕВРОПЕЙСКИ ПЕЧАТ ЗА ЗАЩИТА НА ДАННИТЕ

а. Критериите предвиждат ли да бъдат обхванати всички държави членки?

б. Могат ли критериите да вземат под внимание законодателството или сценариите на държавите членки в областта на защитата на данните?

в. Критериите изискват ли оценка на отделния ОнО по отношение на законодателството на държавите членки в областта на защитата на данните в отделните сектори?

г. Критериите изискват ли администраторът или обработващият лични данни да предостави информация на субектите на данни и на заинтересованите страни на езиците на държавите членки

д. относно обработването/ОнО?

е. документация от обработването/ОнО?

ж. резултатите от оценката?

...

14 ЦЯЛОСТНА ОЦЕНКА НА КРИТЕРИИТЕ

а. Критериите обхващат ли напълно обхвата на механизма за сертифициране (т.е. всеобхватни критерии), за да предоставят достатъчно гаранции, че сертифицирането е надеждно?

- *Пример: Ако обхватът на механизма за сертифициране е насочен към операциите за обработване на данни в областта на здравето, следва да се гарантира високо равнище на защита на данните чрез определяне на критерии, които да гарантират например задълбочена оценка и прилагане на принципите за защита на неприкосновеността на личния живот още при проектирането и по подразбиране.*

б. Критериите съобразени ли са с обхвата на операцията по обработване, която се разглежда с обхвата на механизма за сертифициране, чувствителността на информацията и риска от обработването?

в. Има ли вероятност критериите да подобрят спазването от страна на администраторите и обработващите лични данни на изискванията във връзка със защитата на данните?

г. Дали ще има ползи за субектите на данни по отношение на техните права на информация, включително разясняване на желаните резултати на субектите на данни?