Становище 17/2020 относно проекта на стандартни договорни клаузи, внесен от словенския надзорен орган (член 28, параграф 8 от ОРЗД)

Прието на 19 май 2020 г.

СЪДЪРЖАНИЕ

Европейският комитет по защита на данните

като взе предвид член 28, параграф 8, член 63 и член 64, параграф 1, буква г), параграфи 3—8 от Регламент 2016/679/ЕС на Европейския парламент и на Съвета от 27 април 2016 година 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-долу „ОРЗД“),

като взе предвид Споразумението за Европейското икономическо пространство, и по-конкретно приложение XI и протокол 37 към него, изменени с Решение на Съвместния комитет на ЕИП № 154/2018 от 6 юли 2018 г.,[1]

като взе предвид членове 10 и 22 от своя Правилник за дейността от 25 май 2018 г.,

като има предвид, че:

1) Главната роля на Европейския комитет по защита на данните (по-нататък „Комитетът“) е да гарантира съгласуваното прилагане на ОРЗД в целия Съюз. За тази цел, Комитетът издава становище, основаващо се на член 64, параграф 1, буква г) от ОРЗД, когато надзорен орган (по-нататък „НО“) има за цел да определя стандартни договорни клаузи (по-нататък и „СДК“) съгласно член 28, параграф 8 от ОРЗД. Поради това, целта на настоящото становище е да допринесе за използването на хармонизиран подход относно приемането на мерки от надзорен орган, целящи да породят правни последици по отношение на операции по обработване на данни, които засягат съществено значителен брой субекти на данни в няколко държави членки и съгласуваното прилагане на специфичните разпоредби на ОРЗД.

2) Във връзка с отношенията между администратор на данни и обработващ лични данни (или обработващи лични данни), за обработването на лични данни в член 28 от ОРЗД е определен набор от изисквания, които задължително следва да бъдат включени в конкретен договор между участващите страни .

3) Съгласно член 28, параграф 3 от ОРЗД, обработването от страна на обработващия лични данни *„се урежда с договор или с друг правен акт съгласно правото на Съюза или правото на държава членка, който е задължителен за обработващия лични данни спрямо администратора“*; следователно се определя набор от конкретни аспекти за уреждане на договорните отношения между страните, включително, наред с другото, предмета и продължителността на обработването, неговото естество и цел, типа лични данни, и категориите на субектите на данни.

4) Съгласно член 28, параграф 6 от ОРЗД, без да се засягат разпоредбите на индивидуален договор между администратора на данни и обработващия лични данни, договорът или другият правен акт, посочени в член 28, параграфи 3 и 4 от ОРЗД, може да се основават изцяло или

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

частично на стандартни договорни клаузи. Тези стандартни договорни клаузи трябва да се приемат по отношение на въпросите, посочени в параграфи 3 и 4.

5) Освен това, в член 28, параграф 8 от ОРЗД е определено, че надзорният орган може да приема набор от стандартни договорни клаузи в съответствие с механизма за съгласуваност, посочен в член 63. В този смисъл, надзорните органи са задължени да си сътрудничат с други членове на Комитета и, ако е целесъобразно, с Европейската комисия посредством механизма за съгласуваност. Съгласно член 64, параграф 1, буква г) надзорните органи са задължени да съобщават на Комитета за всеки проект на решение, чиято цел е да се определят стандартни договорни клаузи съгласно член 28, параграф 8. В тази връзка, Комитетът е задължен да издаде становище по въпроса съгласно член 64, параграф 3, в случай че все още не е давал становище по същия въпрос.

6) Приетите стандартни договорни клаузи представляват набор от гаранции, които трябва да се използват, без да се променят, тъй като са предназначени за защита на субектите на данни и за смекчаване на специфичните рискове, свързани с основните принципи на защитата на данни.

7) Становището на Комитета се приема съгласно член 64, параграф 3 от ОРЗД заедно с член 10, параграф 2 от Правилника за дейността на Европейския комитет по защита на данните в рамките на осем седмици от първия работен ден, след като председателят и компетентният надзорен орган са решили, че досието е пълно. По решение на председателя този срок може да бъде удължен с още шест седмици поради сложното естество на въпроса.

ПРИЕ СЛЕДНОТО СТАНОВИЩЕ:

1 ОБОБЩЕНИЕ НА ФАКТИТЕ

1. Словенският надзорен орган (по-нататък „словенският НО“) предостави своя проект на решение и проект на стандартни договорни клаузи на Комитета, като поиска становището му съгласно член 64, параграф 1, буква г) с оглед прилагането на съгласуван подход на равнището на Съюза. Решението относно пълнотата на досието е взето на 21 февруари 2020 г. На 21 февруари 2020 г. секретариатът на ЕКЗД изпрати досието до всички членове от името на председателя.

2. Комитетът получи проекта на СДК от словенския надзорен орган заедно с проект на решение с обяснение за съдържанието и структурата на стандартните договорни клаузи. Тези два документа бяха предоставени от словенския надзорен орган във версия на английски език.

3. В съответствие с член 10, параграф 2 от Правилника за дейността на Комитета[2], поради сложното естество на разглеждания въпрос, Председателят реши да удължи първоначалния срок за приемане от осем седмици с още шест седмици (до 29 май 2020 г.).

[2] Вариант 6, в последно изменената му версия, приет на 29 януари 2020 г.

2 ОЦЕНКА

2.1 Обща обосновка на Комитета относно набора от договорни клаузи

4. Във всеки набор от стандартни договорни клаузи, представен на Комитета съгласно член 28, параграф 8 и член 64, параграф 1, буква г), трябва допълнително да са определени изискванията, предвидени в член 28 от ОРЗД. Становището на Комитета има за цел да се осигури съгласуваност и правилно прилагане на член 28 от ОРЗД по отношение на представените проекти на клаузи, които биха могли да послужат като стандартни договорни клаузи в съответствие с член 28, параграф 8.

5. Комитетът отбелязва, че проектът на СДК, представен на Комитета, се състои от две части:

   1) обща част, в която се съдържат общи разпоредби, които трябва да се използват, без да се променят; и

   2) специфична част, която трябва да се попълни от страните във връзка със конкретното обработване, което трябва да се уреди чрез договора.

6. В допълнение, в своя проект на решение словенският надзорен орган обяснява, че в модела на договор (СДК) „са разгледани основните въпроси, които се обсъждат често от администраторите на данни и обработващите данни при определянето на взаимните им права и задължения“, и, по-конкретно, в него „е разгледано най-вече съдържанието, изложено в член 28, параграф 3 на ОРЗД“, но „са разгледани и въпроси, които могат, в съответствие с опита [им], да породят несигурност сред страните и се нуждаят от специално внимание“.

7. Сред елементите, които трябва да бъдат взети под внимание от Комитета, е факта, че в своето искане словенският надзорен орган посочва пред членовете на ЕКЗД, че е последвал примера на СДК, представени от датския надзорен орган[3] и е взел под внимание Становище 14/2019 на ЕКЗД, прието от ЕКЗД на 9 юли 2019 г.[4]. Комитетът признава, че словенският надзорен орган е взел под внимание посоченото становище, което вече е прието от Комитета, относно проекта на СДК за целите на съответствието с член 28 от ОРЗД, и припомня, че оценката на всеки проект на решение, предмет на механизма за съгласуваност, се извършва индивидуално и сама за себе си, като се вземе предвид стремежа за осигуряване на съгласуваност.

8. Когато в становището не се разглеждат една или повече клаузи на СДК, подадени от словенския надзорен орган, това означава, че Комитетът не иска от словенския надзорен орган да предприеме допълнителни действия във връзка с тези конкретни клаузи.

[3] Окончателната версия на стандартните договорни клаузи за целите на съответствието с член 28 от ОРЗД, приета от датския надзорен орган, е достъпна на адрес: https://edpb.europa.eu/our-work-tools/our-documents/decision-sa/dk-sa-standard-contractual-clauses-purposes-compliance-art_bg.

[4] Становище 14/2019 на ЕКЗД относно проекта на стандартни договорни клаузи, внесен от датския надзорен орган (член 28, параграф 8 от ОРЗД), прието на 9 юли 2019 г., достъпно на адрес: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_bg.pdf.

2.2 Анализ на проекта на стандартни договорни клаузи

2.2.1 Обща бележка относно целите СДК

9. Тъй като в договора съгласно член 28 от ОРЗД следва да бъде посочено и пояснено как ще се изпълнят задълженията, посочени в член 28, параграфи 3—4, е необходимо СДК да бъдат анализирани в тяхната цялост.

10. В допълнение, Комитетът припомня, че възможността за използване на стандартни договорни клаузи, приети от надзорен орган, не пречи страните да добавят други клаузи или допълнителни гаранции, при условие че те не противоречат пряко или косвено на приетите стандартни договорни клаузи или че не накърняват основните права или свободи на субектите на данни. Освен това, ако стандартните клаузи за защита на личните данни бъдат изменени, вече няма да се счита, че страните са приложили приетите стандартни договорни клаузи.

2.2.2 Преамбюл (клауза 1 от СДК)

11. По отношение на **клауза 1.5** от СДК, Комитетът отбелязва, че чрез стандартните договорни клаузи, приети за целите на член 28, се преследват и други цели. Поради това Комитетът насърчава словенския надзорен орган да измени изречението, както следва: „*Клаузите са предназначени за защита на правата на субектите на данни, смекчаване на специфични рискове за защитата на данни и осигуряване на яснота в отношенията между администратора и обработващия данни, както и по отношение на съответните права и задължения*“.

2.2.3 Обработващият лични данни действа според нареждането (клауза 3 от СДК)

12. По отношение на **клауза 3.1** от СДК, Комитетът насърчава словенския надзорен орган да добави думата „или“ в „право на държава членка [или] на Съюза“.

13. В **клауза 3.3** от СДК е посочено, че „*[о]бработващият лични данни и — когато това е приложимо — представителят на обработващия лични данни ще поддържа в съответствие с член 30, параграф 2 от ОРЗД регистър на всички категории дейности по обработването, извършени от името на администратор*“. Въпреки че в член 28, параграф 3 от ОРЗД няма наложено конкретно задължение за администраторите и обработващите данни да включат в договора задължението за обработващия данни да поддържа регистър съгласно член 30, параграф 2 от ОРЗД, Комитетът счита, че тази мярка допринася „за демонстриране на съответствие“ и е от полза за „подпомагане на администратора да гарантира съответствие със задълженията съгласно членове 32—36“ (член 28, параграф 3, букви з) и е) от ОРЗД).

2.2.4 Поверителност (клауза 4 от СДК)

14. Комитетът разбира, че **клауза 4.2** на СДК се отнася до възможността администраторът да поиска от обработващия данни да докаже, че лицата под негово ръководство, които имат достъп до лични данни, са обвързани от задължение за поверителност и получават достъп до лични данни единствено на основа „необходимост да се знае“. Следователно, Комитетът насърчава словенския надзорен орган да направи леко изменение на клаузата, за да я поясни. Тази клауза би могла например да се преформулира, както следва: „*По искане на администратора на*

данни обработващият лични данни доказва, че въпросните лица под ръководството на обработващия лични данни са предмет на горепосоченото задължение за поверителност и получават достъп до лични данни единствено на основа "необходимост да се знае".

2.2.5 Сигурност на обработването (клауза 5 от СДК и приложение B.2)

15. По отношение на **клауза 5.1** от СДК, Комитетът би искал да изтъкне, че като цяло не е целесъобразно в стандартни договорни клаузи само да се потвърждава съдържанието на разпоредбите на ОРЗД, а следва по-скоро да се посочи конкретното прилагане на съответните задължения. Макар че тази клауза не се счита за проблемна, ЕКЗД насърчава словенския надзорен орган да направи леко изменение в нея (напр. „*Съгласно член 32 от ОРЗД, в който се посочва, че [...], страните прилагат [...]*").

16. По отношение на **клауза 5.3**[5] от СДК, Комитетът я разбира като отнасяща се до оценката на риска, извършена независимо от обработващия данни с цел спазване на член 32 и съображение 83 от ОРЗД. Комитетът насърчава словенския надзорен орган да поясни, че тази оценка се отнася до обработването, поверено на обработващия данни от администратора, и припомня, че администраторът по никакъв начин не е освободен от задълженията си за спазване на членове 25, 32, 35 и 36 от ОРЗД. Клауза 5.3 би могла например да се измени, както следва: „*Съгласно член 32 от ОРЗД обработващият данни оценява също — независимо от администратора на данни — рисковете за правата и свободите на физическите лица, свързани с дейностите по обработването, поверени му от администратора, и прилага мерки за смекчаване на тези рискове. За тази цел администраторът на данни предоставя на обработващия лични данни цялата информация, необходима за определяне и оценяване на тези рискове*".

17. В **Приложение B.2** страните се приканват да посочат мерките за сигурност, които са договорени от страните и трябва да се приложат от обработващия лични данни. Комитетът припомня, че степента на подробност на тази информация трябва да бъде такава, че да позволи на администратора да оцени целесъобразността на мерките и да спази своето задължение за отчетност.

2.2.6 Предаване на данни до трети държави или международни организации (клауза 7 и Приложение B.6 от СДК)

18. Комитетът насърчава словенския надзорен орган да поясни, че думите „трети държави" се отнасят за държави извън ЕИП, а не извън Словения. Това може да бъде изпълнено чрез добавяне в клауза 7.1 на *„[...] трети държави (т.е. държави извън Европейското икономическо пространство) [...]*".

19. По отношение на **клауза 7.3** от СДК, Комитетът насърчава словенския надзорен орган да уточни, че посочването на „разрешението" на администратора не е алтернатива на „документираното

[5] В проекта на клауза 5.3 се посочва: "*Съгласно член 32 от ОРЗД обработващият данни оценява също — независимо от администратора на данни — рисковете за правата и свободите на физическите лица, свързани с обработването, и прилага мерки за смекчаване на тези рискове. За тази цел администраторът на данни предоставя на обработващия лични данни цялата информация, необходима за определяне и оценяване на тези рискове*".

нареждане“, а по-скоро описва възможното съдържание на това нареждане. В допълнение Комитетът насърчава словенския надзорен орган допълнително да поясни връзката между клаузи 7.1, 7.2 и 7.3. Следователно, клауза 7.3 би могла да се преформулира, както следва: „*Без документираното нареждане на администратора на лични данни, напр. предоставянето на разрешение, или специфично изискване съгласно правото на ЕС или на държава членка, на което обработващият лични данни е предмет, в рамките на клаузите обработващият лични данни не може [...]*“.

2.2.7 Подпомагане на администратора на лични данни (клауза 8 и Приложение B.3 от СДК)

20. Комитетът е на мнение, че следва да се избягва всяко посочване на конкретен национален надзорен орган в модел на договор, тъй като идентифицирането на компетентния надзорен орган ще зависи от конкретното разглеждано обработване на данни и от конкретните обстоятелства. Следователно, Комитетът препоръчва посочванията на словенския надзорен орган да бъдат премахнати от **клауза 8.2** и да бъдат заменени в двете точки a. и б. с празно място, придружено от бележка, приканваща страните да посочат компетентния надзорен орган (напр. „*[моля, посочете компетентния надзорен орган]*“).

2.2.8 Уведомяване за нарушение на сигурността на личните данни (клауза 9 от СДК)

21. По отношение на **клауза 9.3** от СДК, Комитетът препоръчва позоваването на клауза 9.2.a да бъде заменено с позоваване на клауза 8.2.a. Освен това Комитетът препоръчва позоваването на Приложение Г в **клауза 9.4** да бъде заменено с позоваване на Приложение B.3, а позоваванията на клаузи 9.1 и 9.2 **Приложение B.3** да бъдат заменени с позовавания на клаузи 8.1 и 8.2.

22. По отношение на **Приложение B.3,** Комитетът насърчава словенския надзорен орган да избягва посочване на „ролята и задълженията на обработващия лични данни“ в бележките, приканващи страните да въведат последващи спецификации, тъй като такава обща формулировка може да доведе до несигурност по отношение на попълването на празните места. Следователно, Комитетът предлага да се посочат стъпките, които трябва да се предприемат от обработващия данни и процедурата, която трябва да се следва при оказването на съдействие на администратора (по отношение на уведомяванията за нарушение на сигурността на личните данни и оценките на въздействието върху защитата на личните данни).

2.2.9 Изтриване и връщане на лични данни (клауза 10 от СДК и Приложение B.4)

23. По отношение на **клауза 10.1** от СДК, Комитетът насърчава словенския надзорен орган да поясни, че обработващият данни следва или да изтрие, или да върне личните данни (и да изтрие копията), освен когато правото на ЕС или на държава членка не изисква последващо съхранение на лични данни от обработващия данни. Тъй като изключението от правното задължение се отнася както за Възможност 1, така и за Възможност 2, формулировката „*освен ако правото на Съюза или правото на държава членка не изисква съхранение на лични данни*“ следва да не бъде в по-тъмен шрифт и да бъде представена по начин, който гарантира, че страните по договора не я разбират единствено като отнасяща се до втората възможност. Комитетът предлага допълнително уточняване на тази формулировка (напр. „*освен ако правото на Съюза или правото на държава членка не изисква съхранение на лични данни от обработващия данни*“).

24. Комитетът препоръчва примера в **Приложение В.4** да не се отнася само за „срок“, но и, алтернативно, за „събитие“ „(ПОСОЧЕТЕ СРОК/СЪБИТИЕ)“), тъй като е възможно възникване на ситуации, в които не е възможно установяване на точна времева рамка, а данните следва да се изтрият след настъпването на конкретно събитие. В допълнение, Приложение В.4 следва да се позовава на клауза 10.1 вместо 11.1.

2.2.10 Одит и проверка (клауза 11 от СДК и Приложения В.7 и В.8)

25. Комитетът препоръчва позоваването на Приложения В.6 и В.7 в **клауза 11.2** да бъдат заменени с позоваване на Приложения В.7 и В.8.

26. В допълнение, Комитетът припомня, че одитите, посочени в член 28, параграф 3, буква з) от ОРЗД, се извършват или от самия администратор, или от друг одитор, оправомощен от администратора. Комитетът препоръчва на словенския надзорен орган да адаптира първия сценарий в **Приложения В.7 и В.8**, за да уточни, че одиторът, който е трета страна, е оправомощен от администратора. Следователно текстът на примерите в Приложения В.7 и В.8 следва да се промени, както следва: „*Обработващият лични данни (ПОСОЧЕТЕ ПЕРИОД) за сметка на (ОБРАБОТВАЩИЯ ДАННИ/АДМИНИСТРАТОРА НА ДАННИ)* ***е обект на (ОДИТ/ПРОВЕРКА)*** *от независима трета страна,* ***оправомощена от администратора****, относно спазването на ОРЗД от обработващия лични данни, приложимите разпоредби на ЕС или на държава членка в областта на защитата на данните и клаузите.* ***Независимият одитор, който е трета страна, ще представи (ДОКЛАД НА ОДИТОР/ДОКЛАД ОТ ПРОВЕРКА).*** *Страните се договарят, че в съответствие с клаузите може да се използват следните видове (ДОКЛАД НА ОДИТОР/ДОКЛАД ОТ ПРОВЕРКА): (ВЪВЕДЕТЕ „ОДОБРЕН“ ДОКЛАД НА ОДИТОР/ДОКЛАД ОТ ПРОВЕРКА) […]*“.

2.2.11 Влизане в сила и прекратяване (клауза 13 от СДК)

27. По отношение на **клауза 13.5** от СДК, Комитетът насърчава словенския надзорен орган да избягва посочването на това като конкретна клауза, тъй като тя включва единствено подписите на страните и предполага, че страните и подписите им следва да са упоменати по един и същи начин (напр. „Име“, „Позиция“, „Дата“, „Подпис“, като се премахне посочването на „Телефонен номер“ и „Електронна поща“, които вече са включени в клауза 14.2).

2.2.12 Лица/точки за контакт на администратора на лични данни и обработващия лични данни (клауза 14 от СДК)

28. Комитетът насърчава словенския надзорен оран да измени клауза 14.1, както следва: „*Всяка страна определя отговорно лице за изпълнението на договора*“.

2.2.13 Приложение А

29. Като отбелязва, че Приложение А има за цел предоставяне на подробна информация относно дейностите по обработване, предприети от обработващия лични данни от името на администратора на лични данни, Комитетът припомня, че дейностите по обработване следва да се опишат от страните възможно най-подробно. Поради това е важно примерите, предоставени, за да демонстрират възможното съдържание на разделите на приложението, да могат да насочват страните.

30. С оглед на горепосоченото, Комитетът приветства инициативата на словенския надзорен орган да включи в **Приложение А.4** примери, като дори предлага допълнителното му разширяване, като отчита, че повечето дейности по обработване включват няколко категории субекти на данни едновременно, които от своя страна могат да бъдат категоризирани по няколко начина, напр. потребители, клиенти (възрастни/деца), външни доставчици.

2.2.14 Приложение Б

31. Комитетът насърчава словенския надзорен орган да поясни, че страните могат да посочат множество подизпълнители, обработващи лични данни, в **Приложение Б.1,** макар че в примера е включено само едно поле.

3 ЗАКЛЮЧЕНИЯ

32. Комитетът приветства инициативата на словенския надзорен орган да внесе за становище своя проект на СДК, като това становище има за цел да допринесе за хармонизираното прилагане на ОРЗД.

33. Комитетът е на мнение, че проектът на СДК на словенския надзорен орган, внесен за становище, се нуждае от някои допълнителни корекции, за да бъде счетен за стандартни договорни клаузи. Ако всички посочени в становището препоръки бъдат изпълнени, словенският надзорен орган ще може да използва настоящия проект на споразумение като стандартни договорни клаузи съгласно член 28, параграф 8 от ОРЗД, без да е необходимо последващо приемане от Европейската комисия..

4 ЗАКЛЮЧИТЕЛНИ ЗАБЕЛЕЖКИ

34. Настоящото становище е предназначено за Informacijski pooblaščenec (словенския надзорен орган) и ще бъде публикувано съгласно член 64, параграф 5, буква б) от ОРЗД.

35. Съгласно член 64, параграфи 7 и 8 от ОРЗД надзорният орган трябва да информира председателя на Комитета по електронен път в срок от две седмици след получаване на становището дали ще измени или ще запази своя проект на СДК. В същия срок той представя изменения проект на СДК или, като алтернатива, съответните основания, поради които възнамерява да не се съобрази изцяло или отчасти с настоящото становище. Надзорният орган съобщава окончателното решение на Комитета да включи в регистъра решенията, които са били предмет на механизма за съгласуваност, в съответствие с член 70, параграф 1, буква ш) от ОРЗД.

За Европейския комитет по защита на данните

Председател

(Andrea Jelinek)