Становище на Комитета (член 64)

Становище 14/2019 относно проекта на стандартни договорни клаузи, внесен от датския надзорен орган (член 28, параграф 8 от ОРЗД)

Прието на 9 юли 2019 г.

1 СЪДЪРЖАНИЕ

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 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-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 (наричан по-нататък „Комитетът“) е да гарантира съгласуваното прилагане на ОРЗД в цялото Европейско икономическо пространство (ЕИП). За тази цел от член 64, параграф 1, буква г) от ОРЗД следва, че Комитетът издава становище, когато надзорен орган има за цел да определя стандартни договорни клаузи (СДК) съгласно член 28, параграф 8 от ОРЗД. Поради това, целта на настоящото становище е да допринесе за използването на хармонизиран подход относно трансграничното обработване или обработването, което може да засегне свободния поток на лични данни или на физически лица в Европейското икономическо пространство и съгласуваното прилагане на специфичните разпоредби на ОРЗД.

(2) В контекста на отношенията между администратор на данни и обработващ лични данни (или обработващи лични данни), свързани с обработването на лични данни, в член 28 от ОРЗД, е определен набор от разпоредби, отнасящи се до сключването на конкретен договор между участващите страни и задължителни разпоредби, които следва да бъдат включени в него.

(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*, и в който е определен набор от конкретни аспекти за уреждане на договорните отношения между страните. Наред с другото се включват 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 частично на стандартни договорни клаузи. Тези стандартни договорни клаузи трябва да се приемат по отношение на въпросите, посочени в параграфи 3 и 4.

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

(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. Това означава, че 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 още не го е направил.

(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.

ПРИЕ СЛЕДНОТО СТАНОВИЩЕ:

2 ОБОБЩЕНИЕ НА ФАКТИТЕ

1. Компетентният надзорен орган на Дания представи на Комитета своя проект на стандартни договорни клаузи (наричани по-нататък СДК) посредством информационната система за вътрешния пазар (ИСВП) с искане за становище от Комитета съгласно член 64, параграф 1, буква г), за да се осигури съгласуван подход на равнището на Съюза. Решението относно пълнотата на досието бе взето на 4 април 2019 г. На 4 април секретариатът на Комитета изпрати досието до всички членове от името на председателя.

2. Комитетът получи проекта на СДК от датския надзорен орган[2] заедно с писмо с обяснение за структурата на стандартните договорни клаузи. Тези два документа бяха предоставени от датския надзорен орган във версия на английски език. С настоящия документ Комитетът дава своето становище относно версията на английски език на документа, въпреки че Комитетът отбелязва, че СДК са налични и на датски език на уебсайта на датския надзорен орган. Датският надзорен орган следва да се съобрази в максимална степен със становището на Комитета.

3. В съответствие с член 10, параграф 2 от Правилника за дейността на Комитета[3] поради сложното естество на разглеждания въпрос Председателят реши да удължи първоначалния срок за приемане от осем седмици с още шест седмици — до 9 юли 2019 г.).

[2] С израза „споразумение за обработване на данни“ в документа, предоставен на Комитета, датският надзорен орган нарича стандартните договорни клаузи.
[3] Вариант 2, в последно изменената му версия, приет на 23 ноември 2018 г.

3 ОЦЕНКА

3.1 Обща обосновка на Комитета относно набора от договорни клаузи

4. Във всеки набор от стандартни договорни клаузи, представен на Комитета, трябва допълнително да са определени разпоредбите, 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 договорни клаузи в съответствие с член 28, параграф 8 от ОРЗД.

5. Комитетът отбелязва, че представеният на Комитета документ е проект на СДК, съставен 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 към това датският надзорен орган пояснява в писмото си, че клаузите на СДК, които са в по-тъмен шрифт са задължителни и представляват минималните изисквания на договора съгласно член 28 от ОРЗД. Останалите клаузи, макар и да е препоръчително да бъдат включени в СДК, са незадължителни и може да бъдат включени в СДК по преценка на страните.

7. Комитетът е на мнение, че клаузите, които просто потвърждават разпоредбите на член 28, параграфи 3 и 4, не са достатъчни, за да представляват стандартни договорни клаузи. Поради това Комитетът реши да анализира документа в неговата цялост, включително и допълненията към него. Според становището на Комитета, в договора съгласно член 28 от ОРЗД следва допълнително да се посочи и изясни по какъв начин ще бъдат изпълнени разпоредбите на член 28, параграфи 3 и 4. Именно в този контекст са анализирани СДК, представени на Комитета за становище.

8. Когато в становището не се разглеждат една или повече клаузи на СДК, изготвени от датския надзорен орган, това означава, че Комитетът не иска от датския надзорен орган да предприеме допълнителни действия във връзка с тази конкретна клауза. Клаузи 6.4, 9.3 и 14.3 на датските СДК не са задължителни съгласно член 28 и са свързани с търговски аспекти. Поради това Комитетът не счита тези клаузи за част от СДК. От страните зависи дали ще сключат споразумение и по какъв начин ще го сключат.

3.2 Анализ на проекта на стандартни договорни клаузи

3.2.1 Обща бележка относно целите СДК

9. Комитетът е на мнение, че ако СДК съдържат единствено разделите в по-тъмен шрифт, те няма да са достатъчни, за да се считат за СДК, тъй като някои от разделите, които не са почернени, са свързани със задължителните разпоредби съгласно член 28, параграф 3 от ОРЗД. Поради тази причина, Комитетът препоръчва датският надзорен орган да избягва това разграничение, като ясно заяви или в клаузите, или в отделен документ с указания за употребата на тези клаузи, че всички клаузи на СДК заедно с допълненията следва да бъдат включени в СДК, сключени от страните.

10. В допълнение към това, 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.

11. Комитетът отбелязва, че формулировката на няколко клаузи от СДК не отговаря на съответните разпоредби на ОРЗД. Комитетът е отбелязал това в становището си по-долу и препоръчва датският надзорен орган да приведе формулировката на тези клаузи в съответствие със съответните разпоредби на ОРЗД.

3.2.2 Преамбюл относно обработването на лични данни (клауза 2 от СДК)

12. Що се отнася до **клауза 2.3** от СДК, Комитетът е на мнение, че връзката между споразумението за обработване на лични данни и „основното споразумение“ би могла да бъде по-гъвкава. Възможно е да има случаи, в които стандартните договорни клаузи са в отделен документ, включен като част от основното споразумение, и поради тази причина не са необходими отделни СДК. Възможно е да има и ситуации, в които обработването на лични данни, уредено със СДК, не е част от основно споразумение. Поради това, Комитетът насърчава датския надзорен орган да преработи тази клауза, за да се отрази тази гъвкавост. Тази специфична промяна трябва да бъде прилагана във всеки случай, в който в СДК се споменава основното споразумение.

13. Що се отнася до първо изречение от **клауза 2.4** от СДК, Комитетът е на мнение, че в някои ситуации споразумението за обработване на данни може да бъде прекратено преди „основното споразумение“. Комитетът препоръчва датският надзорен орган да добави в края на първото изречение, че споразумението *„по принцип не може да бъде прекратено самостоятелно, освен когато обработването на данни приключи преди прекратяване на основното споразумение или когато са спазени условията за отделно прекратяване на стандартните договорни клаузи, посочени в неговите клаузи относно прекратяването“ (вж. също препоръката относно клауза 14.4 по-долу)*.

3.2.3 Правата и задължения на администратора на данни (клауза 3 от СДК)

14. Що се отнася до **клауза 3.1** от СДК, Комитетът е на мнение, че формулировката „*носи отговорност пред външния свят*“ е подвеждаща. Действително би могло да се разбере, че задълженията спрямо субектите на данни или други заинтересовани страни са възложени единствено на администратора. Комитетът е на мнение, че тази клауза би била по-ясна, ако се направи позоваване на член 24 от ОРЗД и неговия принцип на отчетност. Поради това, Комитетът препоръчва датският надзорен орган да добави такова позоваване.

15. Освен това, що се отнася до клауза 3.1, би било по-добре да се прави позоваване в общия смисъл на приложимото законодателство по въпросите, свързани със защитата на данните, ако е целесъобразно, вместо на специфичен акт. Комитетът препоръчва датският надзорен орган да измени позоваването на Закона за защита на данните. И накрая, Комитетът предлага думите „в рамките на“ да се заменят с „в съответствие със“.

Поради тази причина, Комитетът би предложил като пример следната формулировка:

„1. *Администраторът на данни има отговорността да гарантира, че обработването на лични данни се извършва в съответствие с Общия регламент за защита на данните (вж. член 24 от ОРЗД), приложимите разпоредби на ЕС или държавите членки за защита на данните (), както и настоящите стандартни договорни клаузи*.“

16. Що се отнася до **клауза 3.2** от СДК, Комитетът е на мнение, че тази клауза е неясна, тъй като администраторът вече е определил целите и средствата на дейността по обработване, предмет на СДК. Комитетът препоръчва датският надзорен оран да измени тази клауза, както следва:

17. *„Администраторът на данни има правото и задължението да взема решения относно целите и средствата за обработване на лични данни“*.

18. Що се отнася до **клауза 3.3** от СДК, Комитетът е на мнение, че значението е неясно. Комитетът приема, че идеята на тази клауза е да се гарантира, че дейностите по обработване, за които администраторът на данни желае да ангажира обработващ лични данни, имат правно основание. Ако това е така, Комитетът препоръчва датският надзорен орган да поясни клаузата по съответния начин.

И накрая, Комитетът отбелязва, че в клауза 3.1 от СДК е използвана формулировката „обработване на лични данни“. В клауза 3.3 от СДК е използвана думата „обработване“. Комитетът препоръчва датският надзорен орган да използва еднаква терминология, за да се избягва объркване.

Предвид това, Комитетът би предложил като пример следната формулировка:

„3. *Администраторът на данни има отговорност, наред с другото, да гарантира, че обработването на лични данни, което обработващият лични данни е получил указания да извърши, има правно основание.*“

3.2.4 Обработващият лични данни действа според нареждането (клауза 4 от СДК)

19. Що се отнася до **клауза 4.1** от СДК, Комитетът е на мнение, че следва да се направи позоваване на приложения A и B, тъй като в тях допълнително се конкретизира нареждането на администратора. Комитетът е на мнение, че администраторът може да дава допълнителни инструкции по време на срока на договора, но това нареждане трябва винаги да бъде документирано.

Освен това, Комитетът отбелязва, че тази клауза е вдъхновена от член 28, параграф 3, буква а) от ОРЗД. Поради това, Комитетът би насърчил датския надзорен орган да използва същата формулировка, както тази в ОРЗД.

20. Що се отнася до **клауза 4.2** от СДК, Комитетът е на мнение, че страните следва да предвидят последици и да предоставят решения в случай на незаконно нареждане.

3.2.5 Поверителност (клауза 5 от СДК)

21. Комитетът разбира клауза 5 от СДК като конкретизиране на член 28, параграф 3, буква б) от ОРЗД, в който се посочва, че „*обработващият лични данни гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност*“.

22. Що се отнася до **клауза 5.1** от СДК, думата „понастоящем“ се разбира от Комитета като необходимостта да се запази преразглежданият статут на „упълномощени лица“. Освен това на Комитета не е ясно кой дава разрешение конкретно на тези лица, тъй като достъпът до лични данни трябва да се предоставя на основа „необходимост да се знае“.

23. Що се отнася до **клауза 5.2** от СДК, Комитетът е на мнение, че тази клауза се отнася до принципа на достъп до личните данни на основа „необходимост да се знае“. Комитетът е на мнение, че клаузи 5.1 и 5.2 от СДК могат да се комбинират, както следва:

„Отговорност на обработващия лични данни е да дава достъп на лица под неговото ръководство до обработваните лични данни от името на администратора, единствено, на основа “необходимост да се знае” и на тези, които са поели ангажимент за поверителност или имат подходящо законово задължение за поверителност. Списъкът с лицата, на които е даден достъп, трябва да се преразглежда периодично. Въз основа на въпросния преглед достъпът до лични данни може да бъде оттеглен и в този случай тези лица повече не могат да имат достъп до личните данни.“

24. Що се отнася до **клауза 5.3** от СДК, Комитетът е на мнение, че тя е обхваната от предложената формулировка по-горе и поради това клауза 5.3 може да се заличи.

25. Що се отнася до **клауза 5.4** от СДК, Комитетът препоръчва датският надзорен орган да заличи формулировката „*може*“, тъй като обработващият лични данни трябва да докаже съответствие с изискванията за поверителност. Освен това, Комитетът насърчава датския надзорен орган да приеме по-широка формулировка, когато се позовава на „*служители*“, тъй като под ръководството на обработващия лични данни може да има и други лица, освен обработващите лични данни служители. По-подходяща би била формулировка като „*лице под ръководството на обработващия лични данни*“ или „*лица, назначени пряко или косвено от*“.

3.2.6 Сигурност на обработването (клауза 6 от СДК)

26. Що се отнася до **клауза 6.1** от СДК, Комитетът препоръчва датският надзорен орган да замени думите „*при отчитане на настоящото равнище*“ в началото на изречението с думите „*като се имат предвид достиженията на техническия прогрес*“, каквато е формулировката в член 32, параграф 1 от ОРЗД. Тази специфична формулировка е използвана в ОРЗД, за да се гарантира, че нивото на сигурност, прилагано към обработването на лични данни, винаги е в съответствие с най-новите технологични развития. В предложената от датския надзорен орган формулировка е направено позоваване на текущо равнище, което след 2 години няма да представлява достижение на техническия прогрес.

27. Що се отнася до **клауза 6.2** от СДК, Комитетът разбира, че тази разпоредба се отнася до член 28, параграф 3, буква в) от ОРЗД и че клауза 9.2 се отнася до член 28, параграф 3, буква е) от ОРЗД. Разграничението между двете клаузи и различните задачи на обработващия лични данни обаче не е много ясно. Комитетът припомня, че в член 28, параграф 3, буква е) от ОРЗД се посочва, че обработващият лични данни подпомага администратора да гарантира изпълнението на задълженията съгласно членове 32—36 от ОРЗД, като отчита естеството на обработване и информацията, до която е осигурен достъп на обработващия лични данни.

Комитетът е на мнение, че посочената в първото изречение на клауза 6.2 „оценка на риска“ трябва да се извършва на дейностите по обработване, които администраторът на лични данни ще възлага на обработващия лични данни. Поради тази причина, администраторът на данни следва да предоставя на обработващия лични данни цялата необходима информация, за да

може обработващият лични данни да спазва член 28, параграф 3, букви в) и е) от ОРЗД. Комитетът би желал да изтъкне, че това не освобождава администратора на данни от отговорността да спазва задълженията си съгласно членове 25, 32 или 35—36 от ОРЗД.

В допълнение към това е необходимо краят на първото изречение на клауза 6.2 да бъде преработен, за да бъде в по-голяма степен в съответствие с клауза 9.2 и приложение В2, тъй като за Комитета не е ясно каква е връзката на формулировката „*след което прилага мерки за преодоляване на идентифицирания риск*“ в клауза 6.2 с клауза 9.2 и приложение В2. Комитетът обърна внимание, че в клауза 9.2.а и приложение В2 се разглежда темата за оценка на риска, но не по същия начин, както в клауза 6.2. Съгласно клауза 6.2 оценката на риска трябва да се извършва от обработващия лични данни, докато съгласно клауза 9.2 и приложение В2 оценката на риска трябва да се извършва от администратора на данни. В приложение В2 още е определено, че обработващият лични данни прилага мерки, договорени с администратора.

Що се отнася до приложение В2, Комитетът е на мнение, че формулировката „*Нивото на сигурност отразява*“ би могла да се промени на „*В нивото на сигурност се взема предвид*“. Що се отнася до елементите, които трябва да се вземат под внимание, в член 32, параграфи 1 и 2 от ОРЗД се споменава естеството, обхватът, контекстът и целите на дейността по обработване, както и рисковете за правата и свободите на физическите лица. Това би могло да бъдат елементи, които могат да се споменат, за да се изясни какво се очаква от „*Опишете елементите, които са от основно значение за нивото на сигурност*“.

Поради това, Комитетът препоръчва датският надзорен орган да поясни и да приведе в съответствие клауза 6.2, 9.2 и приложение В2.

3.2.7 Използване на подизпълнители, обработващи лични данни (клауза 7 от СДК)

28. Що се отнася до **клауза 7.2 и 7.5** от СДК, Комитетът препоръчва датският надзорен орган да замени думата „съгласие“ с „разрешение“, тъй като такава е формулировката на член 28, параграф 2 от ОРЗД.

Освен това, Комитетът е на мнение, че би било по-практично да се създадат следните възможности в тази клауза:

„2. *Поради това, обработващият лични данни не ангажира друг обработващ лични данни (подизпълнител) за изпълнението на настоящите стандартни договорни клаузи без предварителното [Възможност 1] специфично разрешение на администратора на данни/[Възможност 2] общото писмено разрешение на администратора на данни.“*

29. Що се отнася до **клауза 7.3 и 7.4** от СДК, Комитетът счита за важно да се добави фактът, че списъкът с подизпълнители, обработващи лични данни, които са приети от администратора при подписване на договора, следва да бъде включен като допълнение към СДК, било то въз основа на общо разрешение или на специфично. Целта на този списък е да се гарантира, че дори и в случай на общо разрешение администраторът на данни остава информиран относно списъка с подизпълнители, както и за последващи промени. Комитетът препоръчва в СДК да се поясни, че списъкът с подизпълнители в приложение Б2 трябва да бъде предоставен както в случаи на общо, така и на специфично разрешение.

Освен това, в приложение Б1 към СДК има примери за клаузи, от които страните могат да избират. Комитетът счита обаче, че би било по-добре такива клаузи да бъдат включени в самите СДК, вместо в приложенията.

И накрая, що се отнася до общото предварително разрешение, Комитетът е на мнение, че всички условия, които обработващият лични данни може да определи за администратора на данни с цел възразяване срещу промените на подизпълнителя(ите), трябва да дават възможност администраторът на практика да упражнява своята свобода на избор и да му позволяват да запази контрола над личните данни. Това предполага също, че администраторът следва да разполага с достатъчно време, за да възразява срещу такава промяна.

Комитетът препоръчва датският надзорен орган да преработи клауза 7.3, за да създаде възможности в рамките на клаузата, които страните по СДК могат да избират, и да включи съдържанието на клаузи 7.4 и 7.5 в клауза 7.3.

Клауза 7.3 би могла да се изготви, както следва:

„3. В случай на общо писмено разрешение обработващият лични данни уведомява в писмена форма администратора на данни за планирани промени във връзка с добавянето или замяната на подизпълнители най-малко [посочете срок] по-рано, с което дава на администратора на данни възможността да възрази срещу такива промени, преди да бъде ангажиран подизпълнител, обработващ данни. В приложение Б могат да се предвидят по-дълги срокове на предизвестие за специфични услуги, възложени на подизпълнител. Списъкът с вече одобрените от администратора на данни подизпълнители може да бъде намерен в приложение Б.“

В случай на специфично предварително разрешение обработващият лични данни ангажира подизпълнител единствено с предварителното разрешение на администратора на данни. Обработващият лични данни подава искането за специфично разрешение най-малко [посочете срок] преди ангажирането на подизпълнител. Списъкът с вече одобрени от администратора подизпълнители може да бъде намерен в приложение Б.“

Тъй като тази възможност е създадена в самия проект на СДК, приложение Б1 може да се заличи. В допълнение към това, Комитетът препоръчва датският надзорен орган да добави възможност за по-дълъг срок на предизвестие в приложение Б.

30. Що се отнася до **клауза 7.6** от СДК, Комитетът разбира, че тази клауза е позоваване на член 28, параграф 4 от ОРЗД. Както беше посочено по-рано, би било по-добре да се използва точната формулировка на текста от ОРЗД, за да се избегне объркване.

Що се отнася до **клауза 7.8** от СДК, Комитетът би желал да подчертае факта, че неговото съдържание не се изисква съгласно член 18 от ОРЗД. Комитетът е на мнение, че думите „трета страна“ са неясни. Ако намерението е да се създаде „право на трета страна — получател“ за администратора на данни в договора между обработващия лични данни и подизпълнителя, обработващ лични данни, това следва да се посочи.

По мнението на Комитета, добавянето на такава клауза като част от стандартните договорни клаузи повишава стойността им. Действително с нея се запазват правата на администратора на данни, включително отговорността му. Поради тази причина Комитетът насърчава датския надзорен орган да посочи по-ясно, че намерението е да се създаде „право на третата страна получател“ за администратора. Това би предполагало например, че подизпълнителят би приел да бъде отговорен пред администратора на данни, в случай че първоначалният обработващ лични данни изпадне в несъстоятелност, или възможността администраторът на данни да разпорежда пряко на подизпълнителя да върне данните.

31. Що се отнася до **клауза 7.9** от СДК, Комитетът е на мнение, че е важно да се споменат правата на субекта на данни. Това споменаване може да бъде по следния начин: *„Това не засяга правата на субектите на данни по линия на ОРЗД — по-специално тези, които са предвидени в членове 79 и 82 от ОРЗД — срещу администратора на лични данни и обработващия лични данни, включително и подизпълнителя.“*

3.2.8 Предаване на данни до трети държави или международни организации (клауза 8 от СДК)

32. Що се отнася до заглавието на клаузата, Комитетът е на мнение, че то следва да се поясни, че думите „трети държави“ се отнасят до държави извън ЕИП, а не извън Дания. Комитетът насърчава датския надзорен орган да изясни това.

33. Комитетът е на мнение, че в раздел 8 следва да се поясни, че администраторът на лични данни трябва да реши дали предаването е разрешено съгласно договора, или следва да се забрани. Комитетът препоръчва на датския надзорен орган това да се поясни в стандартните договорни клаузи и го насърчава да посочи това в приложение B5.

34. Що се отнася до **клауза 8.1** от СДК, Комитетът отбелязва, че датският надзорен орган е добавил скоби след думата „предаване“ в смисъл на „(прехвърляне, оповестяване и вътрешна употреба)“. Комитетът се колебае дали това е с цел да се даде определение на думата „предаване“. Ако това е целта, Комитетът е на мнение, че тъй като ОРЗД не съдържа такова определение за понятието за предаване, е по-добре термините в скоби да се заличат.

    И накрая, Комитетът препоръчва датският надзорен орган да добави в началото на клауза 8.1 *„В съответствие с глава V от ОРЗД...“* Действително, Комитетът припомня, че за всяко предаване извън ЕС трябва да са спазени всички разпоредби от глава V от ОРЗД. В клауза 8 следва да се изясни, че тези СДК не могат да се разбират като отговарящи на изискванията по член 46 от ОРЗД и поради това не могат да се използват като инструмент за изпълняване на международни предавания по смисъла на глава V от ОРЗД. Това би могло да бъде допълнително отразено в заглавието на клауза 8, което иначе може да създаде впечатлението, че предаванията може да се извършват въз основа на тези СДК.

35. Що се отнася до **клауза 8.2** от СДК, Комитетът има няколко забележки.

    Първо, в началото на изречението Комитетът насърчава датския надзорен орган да добави думата „документирано“ преди „нареждане“, за да гарантира правна сигурност и съответствие с член 28, параграф 3, буква а) от ОРЗД, както и да промени думата *„одобрение“* на *„разрешение“* в съответствие с термините, използвани в член 28 от ОРЗД. Началото на изречението следва да бъде *„Без документираното нареждане или разрешението на администратора на лични данни“.*

    Второ, относно клауза 8.2.а думата *„оповестяване“* може да създаде объркване с понятието за предаване. Освен това, личните данни могат да бъдат предавани на администратор на данни (както вече е посочено в клаузата), но и на обработващ лични данни в трета държава. Комитетът препоръчва датският надзорен орган да изготви клауза 8.2, както следва: *„прехвърляне на лични данни на администратор на данни или на обработващ лични данни в трета държава или в международна организация“*.

Трето, относно клауза 8.2.б думата „прехвърляне“ може да създаде объркване с понятието за предаване. Комитетът препоръчва датският надзорен орган да замени думата „прехвърляне“ с думата „предаване“.

И накрая, относно клауза 8.2.в, за Комитета не е ясно какво е значението на думата „отдели“. Комитетът насърчава датския надзорен орган да замени клауза 8.2.в със следното изречение: „*данните да бъдат обработени от обработващия лични данни извън ЕИП*“.

36. Що се отнася до **клауза 8.3** от СДК, Комитетът разбира, че това е начин нареждането на администратора на данни да бъде документирано в приложение B5. Както вече беше посочено в началото на становището му, Комитетът счита приложенията за задължителни. Комитетът обаче е на мнение, че споменаването на избора на инструмент за предаването би било от полза в допълнение към нареждането, тъй като допринася да се докаже спазването от страните на глава V от ОРЗД. Комитетът насърчава датския надзорен оран да измени клауза 8.3, както следва:

37. „*Нареждането на администратора на лични данни относно предаванията на лични данни на трета държава, включително, ако е приложимо, инструмента за предаване, въз основа на който се извършват тези предавания, е изложено в приложение B5 от настоящите стандартни договорни клаузи. Същата процедура се прилага за одобряването на предавания на лични данни на трета държава.*“

3.2.9 Подпомагане на администратора на лични данни (клауза 9 от СДК)

38. **Клауза 9.1** от СДК отразява съдържанието на член 28, параграф 3, буква д) от ОРЗД. Задължението на обработващия лични данни съгласно тази клауза е да помага на администратора на лични данни да отговаря на искания за упражняване на права на субект на данни. Съдействието може да бъде под различни форми. Комитетът е на мнение, че е необходимо в СДК да се съдържа подробна информация за начина, по който обработващият лични данни е длъжен да предоставя съдействие, а не само списък с възможни за упражняване права.

По-специално, в СДК следва да бъдат изложени стъпките, които обработващият лични данни трябва да предприеме, в случай че получи искане от субект на данни, свързано с упражняването на неговите/нейните права. Например, в такъв случай от споразумението трябва да става ясно дали на обработващия лични данни е забранено да има контакт със субектите на данни и по какъв начин обработващият лични данни трябва да информира администратора, когато става въпрос за правата на субектите на данни (напр. препращане на искането до администратора в определен срок или други подходящи мерки). В такъв случай, съдействието се предоставя единствено чрез обмен на информация между администратора на лични данни и обработващия лични данни. Друг сценарий би могъл да бъде този, при който администраторът на лични данни нарежда на обработващия лични данни да отговори на исканията на субекта на данни според даденото нареждане. Друга възможност би могла да бъде обработващият лични данни да изпълни техническите мерки, указани от администратора на данни, във връзка с правата на субекта на данни. Комитетът препоръчва датският надзорен орган да обмисли възможността да включи следното изречение в клауза 9.1 от СДК:

„*Страните определят в приложение B подходящите технически и организационни мерки, с които обработващият лични данни е задължен да подпомага администратора на лични*

данни, както и обхвата и степента на исканата помощ. Това се отнася за задълженията, предвидени в клаузи 9.1 и 9.2 от стандартните договорни клаузи.“

Необходимо е да се създаде нова точка в приложение B, за да се конкретизират техническите и организационните мерки.

Освен това, Комитетът препоръчва относно клаузи 9.1.а и 9.1.б датският надзорен орган да използва думите *„право да бъде информиран“* вместо думата *„уведомление“*, както следва: *„Право да бъде информиран при събиране на лични данни от субекта на данни“ — Право да бъде информиран, когато личните данни не са получени от субекта на данни“.*

Що се отнася до клауза 9.1.й, Комитетът би предпочел да се използва точната формулировка на ОРЗД. Поради тази причина, Комитетът насърчава датския надзорен орган да я преработи, както следва *„правото да не бъде предмет на решение единствено въз основа на автоматично обработване, включително профилиране“*.

39. **Клауза 9.2** от СДК отразява съдържанието на член 28, параграф 3, буква е) от ОРЗД. Поради това, Комитетът препоръчва *„предоставени данни“* да се замени с *„налична информация“*. Задължението на обработващия лични данни съгласно тази клауза е да съдейства на администратора на лични данни за изпълнението на правните задължения, свързани със сигурността, оценката на въздействието върху защитата на данните и предварителното консултиране с надзорните органи. И тук Комитетът отново е на мнение, че СДК е необходимо да съдържа подробна информация за начина, по който обработващият лични данни е длъжен да оказва съдействие на администратора на лични данни.

Както вече беше посочено в параграф 27 от настоящото становище, датският надзорен орган следва да изясни връзката между клауза 9.2 и клауза 6 относно сигурността на обработването. Комитетът разбира връзката между тези две клаузи като позоваване на член 28, параграф 2, буква в) от ОРЗД за клауза 6 и на член 28, параграф 3, буква е) за клауза 9.2. Действително, клауза 9.2.а и в определена степен клауза 9.2.б са задължения, които обработващият лични данни, предмет на ОРЗД, трябва при всички случаи да изпълни. Това следва от член 32, параграф 1 и член 33, параграф 2 от ОРЗД. За да се запази клауза 9.2.а, ще е необходимо допълнително привеждане в съответствие с член 32, параграф 1 от ОРЗД. Комитетът препоръчва на датския надзорен орган да изясни, че рискът би бил „за правата и свободите на физическите лица“. Освен това трябва да се вземе предвид не само естеството на обработването, но и достиженията на техническия прогрес, разходите за прилагане, обхватът, контекстът и целите на обработването. Комитетът разбира, че страните следва да посочат в приложение B2 минималното ниво на сигурност и мерките, които трябва да приложи обработващият лични данни. Комитетът счита, че е важно в нареждането относно приложение B2 да се включи информация относно подпомагането на администратора на лични данни по отношение на сигурността на обработването.

Комитетът предостави предложение за изменение, което обхваща клаузи 9.1. и 9.2 по-горе.

Относно клауза 9.2б Комитетът е на мнение, че следва да се избягва всяко позоваване на специфичен национален надзорен орган в модел на договор. В допълнение думите *„докладва“* следва да се заменят с *„уведомява“*, а *„разкрие“* следва да се замени със *„след като узнае“*, за да бъдат в съответствие с член 33, параграф 2 от ОРЗД.

Клауза 9.2.б би могла да се изготви, както следва: *„б. неговото задължение, освен ако има вероятност нарушението на личните данни да породи риск за правата и свободите на*

физическите лица, да докладва нарушения на сигурността на личните данни на компетентния надзорен орган [МОЛЯ, ПОСОЧЕТЕ компетентния надзорен орган], без ненужно забавяне и, ако е възможно, не по-късно от 72 часа, след като узнае за такова нарушение".

Относно клауза 9.2.д, Комитетът отново е на мнение, че позоваването на датския надзорен орган следва да се премахне. Клауза 9.2е би могла да се изготви, както следва: *„в. задължението да се консултира с компетентния надзорен орган [ПОСОЧЕТЕ компетентния надзорен орган] преди обработването, когато в оценка на въздействието върху защитата на личните данни е посочено, че обработването би породило висок риск при липсата на мерки, взети от администратора на лични данни, за смекчаване на риска".*

Комитетът счита за важно тази клауза да бъде разгледана по-подробно в приложение В или Г, за да се гарантира, че страните ще вземат мерки относно начина, по който тази помощ се предоставя на практика.

3.2.10 Уведомяване за нарушение на сигурността на личните данни (клауза 10 от СДК)

40. Що се отнася до **клауза 10.1** от СДК, Комитетът, както вече беше заявено, предпочита формулировката на ОРЗД, за да се избегне объркване. В тази клауза думата „откриване" следва да се промени на „след като узнае". В допълнение към това, Комитетът насърчава датския надзорен орган да добави израза „което и да е" пред „нарушение на сигурността на личните данни", за да поясни, че не обработващият лични данни оценява дали компетентният надзорен орган трябва да се уведоми за нарушението на сигурността на личните данни. Това е отговорност на администратора на лични данни[4].

Изречението би могло да се промени, както следва: *„1. В случай на нарушение на сигурността на личните данни обработващият лични данни или подизпълнителят, обработващ лични данни, уведомява администратора без ненужно забавяне, след като е разбрал за него."*

Комитетът препоръчва да се заличи *„в помещенията на обработващия лични данни или на подизпълнителя, обработващ лични данни",* с което задължението за уведомяване би било ограничено до случаите, в които възниква нарушение в тези помещения, докато такова ограничение не произхожда от ОРЗД.

Относно втората част от клауза 10.1 Комитетът е на мнение, че тя може да се допълни, както следва:

„Уведомяването на администратора от обработващия лични данни се извършва, ако е възможно, в рамките на [брой часове], след като обработващият лични данни е разбрал за нарушението, за да се даде възможност на администратора да спази своето задължение за докладване на нарушения на лични данни, което вече е посочено в клауза 9.2.б. "

[4] Вж. Насоките относно уведомяването за нарушения на сигурността на личните данни (стр. 13) „Следва да се отбележи, че не е необходимо обработващият лични данни да извърши първо оценка на вероятността за риск, породен от нарушение, преди да уведоми администратора; именно администраторът трябва да извърши тази оценка, след като е „узнал" за нарушението. Обработващият лични данни е длъжен само да установи дали е настъпило нарушение и след това да уведоми администратора."

41. Що се отнася до **клауза 10.2** от СДК, Комитетът е на мнение, че думите „при отчитане на естеството на обработването и наличната информация“ биха могли да се конкретизират допълнително в приложение Г, за да бъдат по-конкретни и специфични за случая. В нов параграф в края на клауза 10.2 би могло да се добави следната формулировка:

„Страните определят в приложение Г елементите, които обработващият лични данни трябва да предостави, за да подпомогне администратора на лични данни в докладването на нарушение на надзорния орган.“

Освен това, в началото на второто изречение от клауза 10.2, проектът на СДК гласи „*Това може да означава — въз основа на информацията, с която разполага обработващият лични данни — (...)*“. Комитетът е на мнение, че за целите на правната сигурност тази формулировка е по-добре да се избягва. Комитетът насърчава датския надзорен орган да измени тази формулировка, като заличи думата „*може*“.

3.2.11 Изтриване и връщане на лични данни (клауза 11 от СДК)

42. Що се отнася до **клауза 11** от СДК, Комитетът е на мнение, че би било по-практично в тази клауза да се създаде реална възможност. Комитетът насърчава датския надзорен орган да измени тази клауза, за да създаде две конкретни възможности, от които администраторът на лични данни да може да избира.

Тази клауза би могла да се изготви, както следва:

„При прекратяване на дейностите по обработване обработващият лични данни има задължението [Възможност 1] *да заличи всички лични данни, обработени от името на администратора,* [Възможност 2] *да върне всички лични данни на администратора и да заличи съществуващите копия*.

[Незадължително] *Съгласно следното право на ЕС или държавите членки, приложимо към обработващия лични данни, е задължително личните данни да се съхраняват след прекратяване на дейностите по обработване*: ..... Обработващият лични данни се ангажира с изключителното обработване *на данни за целите, предвидени в това право, и при строги приложими условия.“*

Повече информация би могла да се добави в приложение В3, включително относно възможността администраторът на данни да измени опцията, избрана при подписване на договора. Впоследствие, това оказва въздействие върху съдържанието на приложение В. Комитетът насърчава датския надзорен орган да разграничи по-добре периода на съхранение от процедурите по заличаване, заложени в приложение В3 и да отрази възможността администраторът на данни да промени направения избор.

И накрая, Комитетът е на мнение, че думите „дейности по обработване“ трябва да се конкретизират например чрез „след края на предоставянето на услугите, свързани с обработване“. Това може да стане в приложение Г.

3.2.12 Проверка и одит (клауза 12 от СДК)

43. **Клауза 12.1** от СДК отразява съдържанието на член 28, параграф 3, буква з) от ОРЗД. Комитетът препоръчва да се използва същата терминология от параграф 1, „одити, включително проверки“ в параграфи 2 и 3, които се отнасят само до проверката.

44. Що се отнася до **клауза 12.3** от СДК, Комитетът я разбира като обхващаща одит и проверки на подизпълнителя, обработващ лични данни. В съответствие с член 28, параграф 4 от ОРЗД на подизпълнителя се налагат същите задължения, изложени в договора или друг правен акт между администратора и обработващия лични данни. Това включва задължението по член 28, параграф 3, буква з) да се дава възможност за одити от администратора или друг одитор, определен от администратора, и да се допринася за тях. Изготвянето на клауза 12.3 изглежда ограничава това право на администратора на данни спрямо подизпълнителя („ако е приложимо“ и „извършени чрез обработващия лични данни“). Комитетът препоръчва датският надзорен орган да преработи клауза 12.3, за да я приведе в пълно съответствие с ОРЗД. Това може да стане чрез сливане на клаузи 12.2 и 12.3, както следва: „*Процедурите, приложими към одитите на администратора на данни, включително проверки на обработващия лични данни и подизпълнителя, обработващ лични данни, са посочени в* приложения B6 и B7 към *настоящите стандартни договорни клаузи*.“

45. Що се отнася до приложения B6 и B7, Комитетът препоръчва датският надзорен орган да промени следното изречение „*Докладът от проверката се предава без забавяне на администратора на лични данни за информационни цели*“, за да се поясни, че администраторът може да оспорва обхвата, методологията и резултатите от проверката. Администраторът също следва да може да изисква предприемането на мерки вследствие на резултатите от проверката.

46. В допълнение към това, позоваването в приложение B6 на „*Помещенията на обработващия лични данни*“ и B7 на „*Помещенията на подизпълнителя, обработващ лични данни*“, е необходимо да бъде по-обширно. Действително, правата на администратора на данни в рамките на проверките и/или одитите не следва да се ограничават до помещенията на обработващия лични данни или подизпълнителя. Администраторът на данни следва да има достъп до местата, на които се извършва обработването. Това включва физически помещения, както и системи, използвани за обработването и свързани с него.

3.2.13 Споразумение на страните при други условия (клауза 13 от СДК)

47. Що се отнася до **клауза 13** от СДК, Комитетът препоръчва датският надзорен орган да има предвид, че ако бъде включен параграф, в който се посочва отговорност, приложимо право, юрисдикция или други условия, той не може да води до противоречие със съответните разпоредби на ОРЗД или да подкопава нивото на защита, осигурявано от ОРЗД или договора.

3.2.14 Влизане в сила и прекратяване (клауза 14 от СДК)

48. Що се отнася до **клауза 14.4** от СДК, Комитетът е на мнение, че подходяща за СДК може да бъде и специфична разпоредба относно прекратяването на договора. Тъй като позицията на Комитета е, че връзката между споразумението за обработване на данни и основното споразумение следва да бъде по-гъвкава, Комитетът препоръчва датският надзорен орган да включи разпоредба относно прекратяването в рамките на СДК.

49. Що се отнася до **клауза 14.5** от СДК, Комитетът е на мнение, че тази клауза може да е в противоречие с клаузи 2.4 или 14.4. Комитетът препоръчва датският надзорен орган да изясни връзката между тези три клаузи.

3.2.15 Приложение А

50. Приложение А има за цел да даде подробна информация относно дейностите по обработване, извършвани от обработващия лични данни от името на администратора. За тази цел, Комитетът препоръчва целта и естеството на обработването да бъдат описани, както и типа обработвани лични данни, категориите на съответните субекти на данни и продължителността на обработването. Това описание следва да се направи по възможно най-подробен начин, а при всички случаи типовете лични данни трябва да се конкретизират по-добре от просто „лични данни съгласно определението в член 4, параграф 1“ или вместо да се посочва коя категория (членове 6, 9 или 10) лични данни е предмет на обработване. Комитетът е на мнение, че следва да бъде ясно, че в случай на няколко дейности по обработване, тези елементи трябва да бъдат попълнени за всяка от тях. В допълнение към това, Комитетът не е убеден от първите два примера, тъй като е трудно да се разграничи целта от естеството на обработването.

4 ЗАКЛЮЧЕНИЯ

51. Комитетът приветства инициативата на Дания да внесе за становище своя проект на СДК, които имат за цел да допринесат за хармонизираното прилагане на ОРЗД.

52. Комитетът е на мнение, че проектът на СДК на датския надзорен орган, внесен за становище, се нуждае от допълнителни корекции, за да бъде счетен за стандартни договорни клаузи. В становището си по-горе, Комитетът отправи няколко препоръки. Ако всички препоръки бъдат изпълнени, датският 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 Комисията на ЕС.

5 ЗАКЛЮЧИТЕЛНИ ЗАБЕЛЕЖКИ

53. Адресат на настоящото становище е Datatilsynet (датски надзорен орган), като становището ще бъде оповестено публично съгласно член 64, параграф 5, буква б) от ОРЗД.

54. 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 [5] или, ако възнамерява да не се съобрази със становището на Комитета, предоставя съответните основания, поради които възнамерява да не се съобрази изцяло или отчасти с него.

За Европейския комитет по защита на данните

Председател

(Andrea Jelinek)

[5] Надзорният орган съобщава окончателното си решение на Комитета, така че последният да го включи в регистъра на решенията, разгледани съгласно механизма за съгласуваност, в съответствие с член 70, параграф 1, буква ш) от ОРЗД.