Често задавани въпроси относно решението на Съда на Европейския съюз по дело C-311/18 – Комисар по защита на личните данни на Ирландия срещу Facebook Ireland Ltd и Maximillian Schrems

Прието на 23 юли 2020 г.

Настоящият документ има за цел да представи отговори на някои често задавани въпроси, получавани от надзорните органи и ще бъде развиван и допълван с допълнителен анализ в хода на продължаващата работа на Европейския комитет по защита на данните за разглеждане и оценка на решението на Съда на Европейския съюз („Съда“).

Решение C-311/18 можете да откриете тук, а съобщението за медиите, направено от Съда, можете да откриете тук.

1) Какво постанови Съдът в своето решение?

В своето решение, Съдът разгледа валидността на Решение 2010/87/ЕО на Комисията относно стандартните договорни клаузи („СДК“) и счете, че е валидно. В действителност, валидността на това решение не се поставя под въпрос по силата на самото обстоятелство, че стандартните клаузи за защита на данните в това решение, поради техния договорен характер, нямат обвързващо действие за органите на третата държава, към която може да бъдат предадени данните.

Съдът добави обаче, че тази валидност зависи от това дали Решение 2010/87/ЕО включва ефективни механизми, които позволяват на практика да се гарантира спазването на ниво на защита, което по същество е равностойно на това, което се гарантира в рамките на ЕС от Общия регламент относно защитата на данните („ОРЗД“) и че предаването на лични данни в съответствие с такива клаузи се спира или забранява в случай на нарушение на такива клаузи или при невъзможност за спазването им.

В това отношение, Съдът посочи по-специално, че Решение 2010/87/ЕО налага задължение на „износителя на данни“ и получателя на данни („вносител на данни“) да проверява, преди предаването на каквито и да било данни, и да взема предвид по отношение на обстоятелствата на предаването, дали това ниво на защита се спазва в съответната трета държава, както и че Решение 2010/87/ЕО изисква от вносителя на данни да информира износителя на данни ако не може да осигури такова съответствие със стандартните клаузи за защита на данните, а при необходимост – с допълнителните мерки освен тези, включени в клаузата, след

което износителят на данни на свой ред е задължен да спре предаването на данни и/или да прекрати договора с вносителя на данни.

Съдът също така разгледа валидността на Решението относно Щита за личните данни (Решение 2016/1250 относно адекватността на защитата, осигурявана от Щита за личните данни в отношенията между ЕС и САЩ (EU-U.S. Privacy Shield)), тъй като съответните случаи на предаване в контекста на националния спор, довел до искането за преюдициално заключение, се отнасят за предаване между ЕС и Съединените американски щати („САЩ“).

Съдът счете, че изискванията на вътрешното законодателство на САЩ и по-специално на определени програми, които позволяват достъп от страна на публичните органи на САЩ до лични данни, предавани от ЕС към САЩ за целите на националната сигурност, водят до ограничаване на защитата на личните данни, които не са определени по начин, отговарящ на изисквания, които по същество са равностойни на предвидените съгласно правото на Съюза[1] и че това законодателство не предоставя на субектите на данни приложими пред съдилищата права срещу органите на САЩ.

В следствие на тази степен на намеса спрямо основните права на лицата, чиито данни се предават към тази конкретна трета държава, Съдът на ЕС обяви за недействително Решението на ЕК относно Щита за личните данни в отношенията между ЕС и САЩ.

2) Има ли решението на Съда отражение върху инструментите за предаване извън Щита за личните данни?

Като цяло, за третите държави определеният от Съда праг е в сила и за всички подходящи гаранции съгласно член 46 от ОРЗД, които са приложими за предаването на данни от Европейското икономическо пространство (ЕИП) към която и да било трета държава. Посоченото от Съда право на САЩ (т.е. член 702 от Закона за упражняване на надзор върху външното разузнаване („FISA“) и Изпълнителна заповед 12 333) се прилага за всяко предаване на данни към САЩ по електронен път, което попада в обхвата на това законодателство, независимо от конкретното средство, използвано за предаването[2].

3) Има ли някакъв гратисен период, през който мога да продължа да предавам данни към САЩ без да правя оценка на правното основание за предаването?

Не. Съдът обяви за недействително Решението на ЕК относно Щита за личните данни в отношенията между ЕС и САЩ (без продължаване на неговото действие), тъй като оценено от Съда право на САЩ не осигурява ниво на защита, което по своето естество да е равностойно на това в ЕС. Тази оценка трябва да се вземе предвид за всяко предаване към САЩ.

4) Преди предавах данни към вносител на данни в САЩ, който спазваше изискванията на Щита за личните данни. Какво следва да направя сега?

Предаването въз основа на тази правна уредба е незаконно. Ако искате да продължите да предавате данни към САЩ, ще трябва да проверите дали можете да го правите съгласно представените по-долу условия.

5) Използвам СДК с вносител на данни в САЩ. Какво следва да направя?

Съдът установи, че правото на САЩ (т.е. член 702 от FISA и Изпълнителна заповед 12 333) не гарантира ниво на защита, което по същество да е равностойно на това в ЕС.

Дали ще можете да предавате лични данни въз основа на СДК или не ще зависи от резултатите от Вашата оценка, при която трябва да вземете предвид обстоятелствата, свързани с предаването, както и допълнителните мерки, които бихте могли да въведете. Тези мерки в допълнение към СДК, след

---

[1] Съдът подчертава, че определени програми за наблюдение, които позволяват достъп на публични органи на САЩ до лични данни, предавани от ЕС към САЩ, за целите на националната сигурност не осигуряват каквито и да е ограничения върху правомощията, предоставени на органите на САЩ, или гаранции за потенциално обхванати лица, които не са граждани на САЩ.

[2] Член 702 от FISA се прилага за всеки „доставчик на електронни съобщителни услуги“ (вж. определението съгласно Кодекс на САЩ № 50, параграф 1881, буква б), точка 4), а Изпълнителна заповед 12 333 отговаря за организирането на електронното наблюдение, което се определя като „придобиването на непублична комуникация без съгласието на лицето, което видимо присъства на мястото, на което се извършва комуникацията, но без да се включва използване на радиооборудване за локализация единствено за установяване на местоположението на предавателя“ (3.4; б)).

индивидуален анализ във всеки отделен случай на обстоятелствата, свързани с предаването, ще трябва да гарантират, че правото на САЩ не накърнява адекватното ниво на защита, което те обезпечават.

Ако достигнете до заключение, че, вземайки предвид обстоятелствата на предаването на данните и възможните допълнителни мерки, не бихте могли да осигурите подходящи гаранции, сте задължени да прекратите предаването на лични данни. Въпреки това, ако възнамерявате да продължите предаването на данни въпреки това заключение, сте длъжни да уведомите компетентния надзорен орган[3].

6) Използвам задължителни фирмени правила („ЗФП“) по отношение на правен субект в САЩ. Какво следва да предприема?

Предвид решението на Съда на ЕС, с което Решението на ЕК относно Щита за личните данни в отношенията между ЕС и САЩ беше обявено за недействително заради степента на намеса от страна на правото на САЩ спрямо основните права на лицата, чиито данни се предават към тази трета държава, както и обстоятелството, че Щита за личните данни беше предназначен и за предоставяне на гаранции за данните, предавани с други инструменти, като например ЗФП, оценката на Съда се прилага и в контекста на ЗФП, тъй като правото на САЩ има предимство пред този инструмент.

Дали ще можете да предавате лични данни въз основа на ЗФП или не, зависи от резултатите на Вашата оценка, при която трябва да вземете предвид обстоятелствата, свързани с предаването, както и допълнителните мерки, които бихте могли да въведете. Тези мерки, в допълнение към ЗФП, след индивидуален анализ на обстоятелствата, свързани с предаването, във всеки отделен случай, ще трябва да гарантират, че правото на САЩ не накърнява адекватното ниво на защита, което те осигуряват.

Ако резултатите от оценката покажат, че възможните допълнителни мерки предприети във връзка с обстоятелствата по предаването на данните, не биха могли да осигурите подходящи гаранции, Вие сте задължени да прекратите предаването на лични данни. Въпреки това заключение, ако възнамерявате да продължите предаването на данни, сте длъжни да уведомите компетентния надзорен орган[4].

7) Кои са другите възможни инструменти за предаване съгласно член 46 от ОРЗД?

Европейският комитет по защита на данните ще извърши оценка на обстоятелствата на решението във връзка с инструментите извън СДК и ЗФП. В решението се пояснява, че стандартът за подходящи гаранции в член 46 от ОРЗД е за „равностойност по същество“.

Както Съда подчертава, следва да се отбележи, че член 46 се намира в глава V от ОРЗД и в тази връзка трябва да се тълкува в контекста на член 44 от ОРЗД, а именно *„Всички разпоредби на настоящата глава се прилагат, за да се направи необходимото нивото на защита на физическите лица, осигурено от настоящия регламент, да не се излага на риск.“*

8) Мога ли да разчитам на някоя от дерогациите по член 49 от ОРЗД за предаването на данни към САЩ?

Все още е възможно предаване на данни от ЕИП към САЩ въз основа на дерогации, предвидени в член 49 от ОРЗД, при условие, че са приложими условията, предвидени в този член. Европейският комитет по защита на данните се позовава на своите насоки относно тази разпоредба[5].

---

[3] Вж. по-специално съображение 145 от решението на Съда, също клауза 4, буква ж) от Решение 2010/87/ЕО на Комисията, както и клауза 5, буква а) от Решение 2001/497/ЕО на Комисията и Приложение II, буква в) от Решение 2004/915/ЕО на Комисията.

[4] Вж. по-специално съображение 145 от решението на Съда, също клауза 4, буква ж) от Решение 2010/87/ЕО на Комисията. Вж. също така раздел 6.3 WP256 rev.01 (Работна група по чл. 29, работен документ за създаване на таблица с елементите и принципите, които следва да се включват в ЗФП, одобрен от Европейския комитет по защита на данните, http://ec.europa.eu/newsroom/article29/item- detail.cfm?item id=614109) и раздел 6.3 WP257 rev.01 (Работна група по чл. 29, работен документ за създаване на таблица с елементите и принципите, които следва да се включват в ЗФП, одобрен от Европейския комитет по защита на данните, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item id=614110).

[5] Вж. Насоки на Европейския комитет по защита на данните от 2/2018 г. относно дерогациите по член 49 на Регламент 2016/679, приет на 25 май 2018 г., https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018 derogations en.pdf, стр. 3.

По-специално, трябва да се припомни, че когато предаването се извършва въз основа на съгласие от страна на субекта на данни, то следва да бъде:

- изрично,
- специфично за конкретното предаване на данни или съвкупност от предавания (което означава, че износителят на данни трябва да обезпечи получаването на конкретно съгласие преди извършване на предаването, дори ако това се случва след събирането на данните), и
- информирано, по-специално във връзка с възможните рискове за предаването (което означава, че субектът на данни следва да бъде информиран за конкретните рискове, произтичащи от обстоятелството, че неговите данни ще бъдат пренесени към държава, която не осигурява адекватна защита, както и че в нея не се предлагат подходящи гаранции, насочени към осигуряване на защитата на данните)

По отношение на предаване на данни, необходимо за изпълнението на договор между субект на данни и администратор на данни, следва да се има предвид, че лични данни могат да се предават само когато предаването има спорадичен характер. Ще трябва да се установи за всеки отделен случай дали предаването на данни може да се определи като „спорадично“ или „не-спорадично“. Във всеки случай, на тази дерогация може да се разчита единствено когато за предаването има обективна необходимост за изпълнението на договора.

Във връзка с предаване, което се налага от важни причини от обществен интерес (които трябва да се признават от правото на ЕС или на държавите членки), Европейският комитет по защита на данните припомня, че основното изискване за прилагането на тази дерогация е установяването на важен обществен интерес, а не характерът на организацията, както и че макар тази дерогация не се ограничава до предаване на данни със „спорадичен“ характер, това не означава, че предаването на данни въз основа на важния обществен интерес може да се извършва в голям мащаб и систематично. Напротив, трябва да се зачита общия принцип, съгласно който дерогациите, посочени в член 49 от ОРЗД, не следва на практика да се превръщат в „правило“, а вместо това следва да се ограничават до конкретни ситуации и всеки износител на данни следва да се уверява, че предаването отговаря на най-стриктна проверка за необходимост.

9) Мога ли да продължа да използвам СДК и ЗФП за предаване на данни към друга трета държава, различна от САЩ?

Съдът посочи, че по принцип СДК все още може да се използват за предаване на данни към трета държава, но въпреки това прагът, установен от Съда за предаване към САЩ, е приложим и за друга трета държава. Същото е в сила за ЗФП.

Съдът подчерта, че администраторите на лични данни носят отговорност за извършване на оценка дали нивото на защита, което се изисква съгласно правото на ЕС, се спазват в конкретната трета държава, за да се определи дали СДК или от ЗФП могат на практика да се приложат. В случай че това не е така, следва да прецените дали можете да осигурите допълнителни мерки за гарантиране на ниво на защита, което по същество е равностойно на това в ЕИП, както и че правото на третата държава не противоречи на тези допълнителни мерки, което да въздейства на тяхната ефективност.

Можете да се свържете с вносителя на данни, за да проверите правото в конкретната държава и да си сътрудничите за неговата оценка. Ако Вие или вносителят на данни в третата държава прецените, че предаването на данни съгласно СДК или ЗФП не позволява ниво на защита, което по същество да е равностойно на това в ЕИП, следва незабавно да прекратите предаването. В противен случай, трябва да уведомите компетентния надзорен орган[6].

Както беше подчертано от Съда, въпреки че е основно задължение на износителите на данни и вносителите на данни сами да извършват оценка дали законодателството на третата държава дава възможност на вносителя на данни да спази стандартните клаузи за защита на данните или ЗФП, преди осъществяване на предаването на лични данни към тази трета държава, надзорните органи също ще изпълняват ключова роля

[6] Вж. по-специално съображение 145 от решението на Съда на ЕС. Във връзка със СДК, вж. клауза 4, буква ж) от Решение 2010/87/ЕО на Комисията, както и клауза 5, буква а) от Решение 2001/497/ЕО на Комисията и Приложение II, буква в) от Решение 2004/915/ЕО на Комисията. Във връзка със ЗФП, вж. раздел WP256 rev.01 (одобрен от Европейския комитет по защита на данните), както и раздел 6.3 WP257 rev.01 (одобрен от Европейския комитет по защита на данните).

за правоприлагането на ОРЗД и при издаването на допълнителни решения относно предаването на данни към трети държави.

С цел да се избегнат разнородни решения, Съдът призова да се предприемат допълнителни действия от Европейския комитет по защита на данните, за да се гарантира последователност и по-специално дали предаването към трети държави трябва да се забрани.

10) Какъв вид допълнителни мерки мога да въведа, ако използвам СДК и ЗФП за предаване на данни към трети държави?

Допълнителните мерки, които можете да предвидите при необходимост, ще трябва да се предоставят за всеки отделен случай и за тях да се вземат предвид всички обстоятелства на предаването и след оценка на правото на третата държава, за да се провери дали то гарантира адекватно ниво на защита.

Съдът подчерта, че отговорността за извършването на тази оценка и за осигуряването на необходимите допълнителни мерки се носи от износителя и вносителя на данните.

Понастоящем Европейският комитет по защита на данните анализира решението на Съда, за да определи видовете допълнителни мерки, които могат да се предоставят към СДК и ЗФП, с правно, техническо и организационно естество, за предаването на данни към трети държави, в които СДК и ЗФП сами по себе си няма да осигурят достатъчно ниво на гаранции.

Европейският комитет по защита на данните разглежда по-задълбочено в какво могат да се състоят тези допълнителни мерки и ще предостави последващи насоки по въпроса.

11) Как се установява от администратор на лични данни дали обработващ лични данни от негово име предава данните към САЩ или трета държава?

В договора, който сте сключили с обработващия лични данни в съответствие с член 28, параграф 3 от ОРЗД, трябва да се посочва дали се разрешава предаване на данни или не (трябва да се има предвид че дори предоставянето на достъп до данни от трета държава, например за административни цели, представлява форма на предаване).

Предоставяне на разрешение се изисква и по отношение на обработващите лични данни, които възлагат на подизпълнители предаването на данните към трети държави. Трябва да обърнете особено внимание, тъй като различни софтуерни решения могат да осъществяват предаване на лични данни към трета държава (например за целите на съхранението или поддръжката).

12) Какво мога да направя, за да продължа да използвам услугите на моя обработващ лични данни ако в договора, сключен съгласно член 28, параграф 3 от ОРЗД, се посочва, че данните могат да бъдат предавани към САЩ или друга трета държава?

Ако данните, обработвани от Ваше име, могат да бъдат предадени в САЩ, но не могат да бъдат предоставени допълнителни мерки, за да се гарантира, че законодателството на САЩ не засяга по същество равнището на защита, равностойно на това в ЕИП (предоставено от инструментите за трансфер), като също така не са приложими дерогации по член 49 от ОРЗД, единственото решение е да договорите изменение или допълнение към договора, с които да се забранява предаване към САЩ. Данните следва не само да се съхраняват, но и да се обработват на друго място, различно от САЩ.

Ако същите данни могат да бъдат предавани към друга трета държава, трябва да изследвате и законодателството на тази трета държава, за да сте сигурни дали тя спазва изискванията на Съда на ЕС и дали предлага адекватното ниво на защита на личните данни. Ако не откривате подходящо основание за предаване на данни към трета държава, личните данни не трябва да се предават извън територията на ЕИП и всички дейности по обработването им следва да се извършват в рамките на ЕИП.

От името на Европейския комитет по защита на данните, председател, Андреа Йелинек