

Често задавани въпроси относно решението на Съда на Европейския съюз по дело C-311/18 — *Data Protection Commissioner/Facebook Ireland u Maximilian Schrems*

Прието на 23 юли 2020 г.

Настоящият документ има за цел да представи отговори на някои често задавани въпроси, получени от надзорните органи („НО“), и ще бъде разработван и допълван, наред с допълнителен анализ, тъй като ЕКЗД продължава да извършва преглед и оценка на решението на Съда на Европейския съюз („Съдът“).

Решението C-311/18 може да бъде намерено [тук](#), а съобщението за пресата на Съда — [тук](#).

1) Какво е постановил Съдът в решението си?

→ В решението си Съдът разглежда валидността на Решение 2010/87/ЕС на Комисията относно стандартните договорни клаузи („СДК“) и приема, че то е валидно. Валидността на това решение не се поставя под въпрос само поради факта, че съдържащите се в него стандартни клаузи за защита на данните, предвид договорния им характер, не обвързват органите на третите държави, на които могат да се предават данни.

Същевременно, Съдът добавя, че тази валидност зависи от това, дали Решение 2010/87/ЕС съдържа ефективни механизми, позволяващи на практика да се осигури спазването на ниво на защита, което по същество е равностойно на гарантираното в ЕС чрез ОРЗД, и че предаването на лични данни, основаващо се на такива клаузи, ще бъде спряно или забранено в случай на нарушение на тези клаузи или при невъзможност за спазването им.

В тази връзка Съдът посочва по-специално, че Решение 2010/87/ЕС налага задължение за износителя на данните и за получателя на данните („вносителят на данните“) да проверят предварително, като вземат предвид обстоятелствата на предаването, дали в съответната трета държава се спазва ниво на защита, както и че Решение 2010/87/ЕС изисква вносителят на данните да информира износителя на данните за евентуалната си невъзможност да осигури съответствие със стандартните клаузи за защита на данните и когато е необходимо — с допълнителни мерки към предвидените в тези клаузи, като тогава износителят на данните е задължен да спре предаването на данни и/или да прекрати договора с вносителя на данните.

- Съдът разгледа също 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), тъй като въпросните трансфери, които са предизвикали национален спор и са довели до отправено преюдициално запитване са между ЕС и Съединените американски щати („САЩ“).

Съдът приема, че изискванията на вътрешноправната уредба на САЩ и по-специално на определени програми, позволяващи достъп от страна на американските публични органи до личните данни, предавани от ЕС на САЩ за целите на националната сигурност, водят до ограничения на защитата на личните данни, които не са определени по начин, който да отговаря на изисквания, които по същество са равностойни с тези, заложи в правото на ЕС¹, и това законодателство не предоставя на субектите на данни приложими пред съдилищата права срещу американските органи.

Вследствие на тази степен на намеса в основните права на лицата, чиито данни са предадени на посочената трета държава, Съдът обявява Решението относно адекватността на Щита за личните данни за невалидно.

2) Решението на Съда има ли последици за други инструменти за предаване, различни от Щита за личните данни?

- Като цяло, по отношение на трети държави, определеният от Съда праг се прилага и за всички подходящи гаранции по член 46 от ОРЗД, които се използват за предаване на данни от ЕИП на трета държава. Правната уредба на САЩ, посочена от Съда (т.е. член 702 от FISA и EO 12333), се прилага за всяко предаване на САЩ по електронен път, което попада в приложното поле на това законодателство, независимо от използваните инструменти за предаване².

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

- Не, Съдът е обявил Решението относно Щита за личните данни за невалидно, без да се запазва действието му, тъй като преценената от Съда правна уредба на САЩ не предоставя равностойно по същество ниво на защита на ЕС. Тази преценка трябва да се взема предвид за всяко предаване на САЩ.

4) Предавал съм данни на американски вносител на данни в съответствие с Щита за личните данни? Какво трябва да направя сега?

- Предаването на основание на тази правна рамка е незаконно. Ако искате да продължите да предавате данни на САЩ, трябва да проверите дали можете да го правите при посочените по-долу условия.

¹ Съдът подчертава, че определени програми за наблюдение, позволяващи достъп от страна на американските публични органи до личните данни, предавани от ЕС на САЩ за целите на националната сигурност, не предвиждат ограничения на оправомощаването на американските органи, нито съществуването на гаранции за потенциално обхванатите лица, които не са американски граждани.

² Член 702 от FISA се прилага за всички „доставчици на електронна комуникационна услуга“ (вж. определението в 50 USC § 1881(b)(4), докато EO 12 333 организира електронното наблюдение, което означава „придобиване на съобщение по електронен път, което не е обществено достояние, без съгласието на лицето, което е страна по електронната комуникация, или при неелектронна комуникация — без съгласието на лицето, което видимо присъства на мястото, където се извършва комуникацията, с изключение на използването на радиооборудване за ориентиране по посока единствено за установяване на местоположението на предавателя“ (3.4; b).

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

- Съдът е приел, че правната уредба на САЩ (т.е. член 702 от FISA и EO 12333) не осигурява равностойно по същество ниво на защита.

Възможността да предавате лични данни на основание на СДК ще зависи от резултата от оценката Ви, като вземете предвид обстоятелствата на предаването и допълнителните мерки, които можете да въведете. Допълнителните мерки, наред със СДК, установени след анализ на всяко едно обстоятелство, свързано с предаването, трябва да гарантират, че правната уредба на САЩ не засяга осигуреното от тях адекватно ниво на защита.

Ако стигнете до заключение, че с оглед на обстоятелствата на предаването и възможните допълнителни мерки няма да бъдат осигурени подходящи гаранции, трябва да спрете или да прекратите предаването на личните данни. От друга страна, ако възнамерявате да продължите да предавате данни въпреки това заключение, трябва да уведомите компетентния във Вашия случай НО³.

6) Използвам задължителни фирмени правила („ЗФП“) със субект в САЩ. Какво трябва да направя?

- Предвид решението на Съда, с което Щитът за личните данни се обявява за невалиден поради създадената от правната уредба на САЩ степен на намеса в основните права на лицата, чиито данни се предават на тази трета държава, и обстоятелството, че Щитът за лични данни е предназначен също да осигурява гаранции на данните, предавани с други инструменти, например ЗФП, преценката на Съда се прилага и при ЗФП, тъй като правото на САЩ ще има предимство и върху този инструмент.

Възможността да предавате лични данни на основание на ЗФП ще зависи от резултата от оценката Ви, като вземете предвид обстоятелствата на предаването и допълнителните мерки, които можете да въведете. Тези допълнителни мерки, наред със ЗФП, установени след анализ на всяко едно обстоятелство, свързано с предаването, трябва да гарантират, че правната уредба на САЩ не засяга гарантираното от тях адекватно ниво на защита.

Ако стигнете до заключение, че с оглед на обстоятелствата на предаването и възможните допълнителни мерки няма да бъдат осигурени подходящи гаранции, трябва да спрете или прекратите предаването на личните данни. От друга страна, ако възнамерявате да продължите да предавате данни въпреки това заключение, трябва да уведомите компетентния във Вашия случай НО⁴.

7) Какво е положението с другите инструменти за предаване по член 46 от ОРЗД?

³ Вж. по-специално точка 145 от решението на Съда и клауза 4, буква ж) от Решение 2010/87/ЕС на Комисията, както и клауза 5, буква а) от Решение 2001/497/ЕО на Комисията и комплект II, буква в) от приложението към Решение 2004/915/ЕО на Комисията.

⁴ Вж. по-специално точка 145 от решението на Съда и клауза 4, буква ж) от Решение 2010/87/ЕС на Комисията. Вж. също раздел 6.3 РД256, ред.01 (Работна група по член 29, Работен документ за съставянето на таблица с елементите и принципите, които трябва да бъдат заложиени в задължителните фирмени правила, одобрен от ЕКЗД), http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109) и раздел 6.3 РД257, ред.01 (Работна група по член 29, Работен документ за съставянето на таблица с елементите и принципите, които трябва да бъдат заложиени в задължителните фирмени правила за обработващи лични данни, одобрен от ЕКЗД, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110).

- ЕКЗД ще направи оценка на последиците от решението за другите инструменти за предаване, различни от СДК и ЗФП. В решението се пояснява, че стандартът за въвеждане на подходящи гаранции, заложен в член 46 от ОРЗД е „равностоен по същество“.

Както Съдът подчертава, трябва да се отбележи, че член 46 е поместен в глава V от ОРЗД и следователно трябва да се разглежда в светлината на член 44 от ОРЗД, който гласи, че *„всички разпоредби на [тази] 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 използвам една от дерогациите по член 49 от ОРЗД, за да предам данни на САЩ?

- Предаването на данни от ЕИП на САЩ все още е възможно на основание на дерогациите, предвидени в член 49 от ОРЗД, при условие че се прилагат предвидените в този член условия. ЕКЗД посочва тази разпоредба в насоките си⁵.

По-специално трябва да се припомни, че когато предаването се основава на съгласието на субекта на данните, то трябва да бъде:

-) дадено изрично,
-) конкретно за съответното предаване на данни или съвкупност от предавания на данни (в смисъл, че износителят на данни трябва да направи необходимото, за да получи конкретно съгласие, преди да се предадат данните, дори ако това се случи след събирането им) и
-) информирано, особено що се отнася до възможните рискове от предаването на данните (в смисъл, че субектите на данни също трябва да бъдат информирани за специфичните рискове, произтичащи от факта, че техните данни ще бъдат предадени на държава, която не осигурява адекватна защита, и че не се прилагат подходящи гаранции, предназначени да осигурят защита на данните).

Що се касае до предаванията, необходими за изпълнението на договор, сключен между субекта на данните и администратора, трябва да се има предвид, че личните данни могат да бъдат предадени, когато предаването засяга отделни случаи. Трябва да се установи за всеки отделен случай дали предаванията на данни се окачествяват като „засягащи отделен случай“ или „незасягащи отделен случай“. При всички случаи тази дерогация може да се използва, когато предаването е обективно необходимо за изпълнението на договора.

По отношение на предавания, необходими поради важни причини от обществен интерес (които трябва да са признати в правото на ЕС или правото на държавата членка⁶), ЕКЗД напомня, че същественото изискване за приложимостта на тази дерогация е констатирането на важен обществен интерес, а не естеството на организацията, както и че макар тази дерогация да не се ограничава до предаването на данни, „които засягат отделни случаи“, това не означава, че предаванията на данни въз основа на тази дерогация може да се извършват системно и в голям мащаб. По-скоро трябва да бъде спазван общият принцип, според който дерогациите, посочени в член 49 от ОРЗД, на практика не се превръщат в „правило“, а трябва да се ограничават до конкретни ситуации и всеки

⁵ Вж. Насоки № 2/2018 на ЕКЗД относно дерогациите по член 49 на Регламент 2016/679, приети на 25 май 2018 г., https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_bg.pdf, стр. 3.

⁶ Позоваванията на „държави членки“ следва да се разбират като позовавания на „държавите — членки на ЕИП“.

износител на данни трябва да гарантира, че тяхното предаване отговаря на строгия критерий за необходимост.

9) Мога ли да продължа да използвам СДК или ЗФП, за да предавам данни на друга трета страна, различна от САЩ?

- Съдът е посочил, че СДК по правило все още могат да бъдат използвани за предаване на данни на трета държава, но определеният от Съда праг за предавания на САЩ се прилага за която и да е трета държава. Това важи и за ЗФП.

Съдът подчертава, че износителят и вносителят на данни са длъжни да извършат оценка на спазването на изискването от правото на ЕС ниво на защита в съответната трета държава, за да установят дали предвидените в СДК или в ЗФП гаранции могат да бъдат спазени на практика. Ако това не е така, трябва да прецените дали можете да осигурите допълнителни мерки, за да гарантирате същото ниво на защита, като това в ЕИП и дали правото на третата държава няма да засегне тези допълнителни мерки по начин, който нарушава ефективността им.

Може да се свържете със своя вносител на данни, за да проверите законодателството на държавата му и да си сътрудничите при оценката му. Ако Вие или вносителят на данни в третата държава установите, че данните, предавани в съответствие със СДК или ЗФП, не се ползват със същото ниво на защита, като това, което е гарантирано в ЕИП, трябва незабавно да спрете предаванията. Ако не го направите, трябва да уведомите компетентния във Вашия случай НО⁷.

- Въпреки че, както подчертава Съдът, главно износителите и вносителите на данни са длъжни да се уверят, че законодателството на третата държава на местоназначение позволява на вносителя на данни да се съобрази със стандартните клаузи за защита на данните или със ЗФП преди предаването на личните данни на тази трета държава, НО също трябва да имат ключова роля при прилагането на ОРЗД и при издаването на по-нататъшни решения за предаване на трети държави.

Като Съдът ги приканва, те ще си сътрудничат по-нататък с ЕКЗД, за да избегнат различаващи се решения и за да осигурят съгласуваност особено, когато предаванията на трети държави трябва да се забранят.

10) Какви допълнителни мерки мога да въведа, ако използвам СДК или ЗФП, за да предавам данни на трети държави?

- Допълнителните мерки, които можете да предвидите, ако е необходимо, трябва да бъдат заложили за всеки отделен случай при отчитане на всички обстоятелства на предаването и след извършване на оценка на правната уредба на третата държава, за да се провери дали тя гарантира адекватно ниво на защита.

Съдът подчертава, че главно износителят и вносителят на данни са длъжни да извършат тази оценка, както и да предоставят необходимите допълнителни мерки.

ЕКЗД понастоящем анализира решението на Съда, за да определи какъв вид допълнителни мерки правни, технически или организационни биха могли да се предоставят в допълнение

⁷ Вж. по-специално точка 145 от решението на Съда. Във връзка със СДК, вж. клауза 4, буква ж) от Решение 2010/87/ЕС на Комисията, както и клауза 5, буква а) от Решение 2001/497/ЕО на Комисията и комплект II, буква в) от приложението към Решение 2004/915/ЕО на Комисията. Във връзка със ЗФП вж. раздел 6.3 РД256, ред.01 (одобрен от ЕКЗД) и раздел 6.3 РД257, ред.01 (одобрен от ЕКЗД).

към СДК или ЗФП, за да се предават данни на трети държави, когато СДК или ЗФП сами по себе си не предвиждат достатъчно ниво на гаранции.

→ ЕКЗД проучва по-подробно в какво могат да се изразяват тези допълнителни мерки и ще предостави още насоки.

11) Използвам обработващ лични данни, който обработва данни, за които аз съм отговорен като администратор. Как мога да разбера дали този обработващ лични данни предава данни на САЩ или на друга трета държава?

→ Договорът, който сте сключили с Вашия обработващ лични данни в съответствие с член 28, параграф 3 от ОРЗД, трябва да предвижда дали предаванията са разрешени (следва да се има предвид, че дори предоставянето на достъп до данни от трета държава, например за административни цели, също представлява предаване).

→ Обработващите лични данни трябва да имат също разрешение, за да възлагат на подизпълнители предаването на данни на трети държави. Трябва да обръщате внимание и да сте предпазлив/а, тъй като много компютърни решения могат да предполагат предаване на лични данни на трета държава (напр. за съхранение или поддръжка).

12) Какво мога да направя, за да продължа да използвам услугите на моя обработващ лични данни, ако в договора, подписан в съответствие с член 28, параграф 3 от ОРЗД, е посочено, че тези данни могат да бъдат предавани на САЩ или на друга трета държава?

→ Ако данните Ви могат да бъдат предавани на САЩ и не могат да се предвидят никакви допълнителни мерки, за да се гарантира, че правната уредба на САЩ не засяга равностойното по същество ниво на защита, предоставено в ЕИП чрез инструментите за предаване, нито се прилагат дерогациите по член 49 от ОРЗД, единственото решение е да договорите изменение или допълнителна клауза в договора Ви, с цел да се забранят предаванията на САЩ. Данните трябва да бъдат не само съхранявани, но и администрирани извън САЩ.

→ Ако данните Ви могат да бъдат предавани на друга трета държава, трябва да проверите също законодателството на тази трета държава за съответствие с изискванията на Съда и с очакваното ниво на защита на личните данни. Ако не може да се установи подходящо основание за предаванията на трета държава, личните данни не трябва да бъдат предавани извън територията на ЕИП, като всички дейности по обработване трябва да се извършват в ЕИП.

За Европейския комитет по защита на данните

Председател

Andrea Jelinek