

РАМКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ОТНОШЕНИЯТА МЕЖДУ ЕС И САЩ

Ч.З.В. ЗА ЕВРОПЕЙСКИТЕ ПРЕДПРИЯТИЯ¹

Приети на 16 юли 2024 г.

¹ В този смисъл „европейски предприятия“ се отнася до предприятия в ЕИП, които прехвърлят или могат да прехвърлят лични данни на предприятия в САЩ, сертифицирани по РЗЛД.

Съдържание

V1. Какво представлява рамката за защита на личните данни в отношенията между ЕС и САЩ?.....	3
V2. Кои американски дружества могат да се възползват от Рамката за защита на личните данни в отношенията между ЕС и САЩ?.....	4
V3. Какво да направите, преди да прехвърлите лични данни на дружество в САЩ, която е сертифицирано или твърди, че е сертифицирано съгласно Рамката за защита на личните данни в отношенията между ЕС и САЩ?	4
V4. Къде мога да намеря насоки относно сертифицирането на американски дъщерни предприятия на европейски дружества?.....	7

В1. КАКВО ПРЕДСТАВЛЯВА РАМКАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ОТНОШЕНИЯТА МЕЖДУ ЕС И САЩ?

Рамката за защита на личните данни в отношенията между ЕС и САЩ („РЗЛД“) е механизъм за самосертифициране на дружества в САЩ. Предприятията, които се самосертифицират по РЗЛД, трябва да спазват нейните принципи, правила и задължения, свързани с обработването на лични данни на лица от ЕИП. За повече информация относно тези ангажименти вж. [принципите на рамката за защита на личните данни](#).²

Европейската комисия счита, че прехвърлянето на лични данни от ЕИП на дружества, сертифицирани по РЗЛД, се извършва при осигурено адекватно ниво на защита.³ В резултат на това личните данни могат да се трансферират свободно на сертифицирани дружества в САЩ, без да е необходимо да се въвеждат допълнителни гаранции или да се получава разрешение. Ето някои важни връзки за повече информация:

- [Въпроси и отговори](#) на Европейската комисия: [Рамка за личните данни в отношенията между ЕС и САЩ](#)⁴
- [Уебсайтът на рамката за личните данни, управляван от Министерството на търговията на САЩ](#)⁵
- [Решението на Европейската комисия относно адекватното ниво на защита на личните данни съгласно Рамката за защита на личните данни в отношенията между ЕС и САЩ](#)⁶

РЗЛД се прилага за всички видове лични данни, прехвърляни от ЕИП на САЩ, включително лични данни, обработвани за търговски или здравни цели, и данни за човешки ресурси, събрани

²[https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-\(DPF\)-Principles](https://www.dataprivacyframework.gov/program-articles/Participation-Requirements-Data-Privacy-Framework-(DPF)-Principles)

³ Решението относно адекватността на рамката за защита на личните данни е прието от Европейската комисия на 10 юли 2023 г. То е разработено от Европейската комисия и Министерството на търговията на САЩ, за да замени Решение (ЕС) 2016/1250 относно Щита за личните данни, което беше обявено за невалидно от Съда на Европейския съюз на 16 юли 2020 г. по дело C-311/18, *Комисар по защита на данните/Facebook Ireland Limited u Maximilian Schrems (Schrems II)*.

⁴ https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

⁵ <https://www.dataprivacyframework.gov/s/>

⁶ https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

в рамките на трудово правоотношение (наричани по-долу „Данни за ЧР“), при условие че дружеството получател в САЩ е самосертифицирано съгласно РЗЛД, за да обработва тези видове данни.⁷

В2. КОИ АМЕРИКАНСКИ ДРУЖЕСТВА МОГАТ ДА СЕ ВЪЗПОЛЗВАТ ОТ РАМКАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ОТНОШЕНИЯТА МЕЖДУ ЕС И САЩ?

За да отговаря на условията за самосертифициране по РЗЛД, дадено дружество в САЩ трябва да се подчинява на правомощията за разследване и правоприлагане на Федералната комисия по търговия на САЩ (ФКТ) или на Министерството на транспорта на САЩ (МТ). В бъдеще могат да бъдат включени и други уставни органи на САЩ.⁸

Това означава например, че организациите с нестопанска цел, банките, застрахователните дружества и доставчиците на телекомуникационни услуги (по отношение на дейностите на общите превозвачи), които не попадат под юрисдикцията на ФКТ или МТ, не могат да се самосертифицират съгласно РЗЛД.

В3. КАКВО ДА НАПРАВИТЕ, ПРЕДИ ДА ПРЕХВЪРЛИТЕ ЛИЧНИ ДАННИ НА ДРУЖЕСТВО В САЩ, КОЯТО Е СЕРТИФИЦИРАНО ИЛИ ТВЪРДИ, ЧЕ Е СЕРТИФИЦИРАНО СЪГЛАСНО РАМКАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ОТНОШЕНИЯТА МЕЖДУ ЕС И САЩ?

Преди да предаде лични данни на дружество в САЩ, което твърди, че се е самосертифицирало по РЗЛД, износителят на данни в ЕИП трябва да се увери, че то притежава активна самосертификация (сертификатите трябва да се подновяват ежегодно) и че тази сертификация обхваща въпросните данни (по-специално, ако обхваща данни за ЧР, съответно данни, които не са данни за ЧР).⁹

За да проверят дали дадено самосертифициране е активно и приложимо, износителите на данни в ЕИП трябва да проверят дали дружеството в САЩ е в [списъка към рамката за защита на личните данни](#)¹⁰, публикуван на уебсайта на Министерството на търговията на САЩ. Този списък включва и регистър на дружествата, които са заличени от списъка („неактивни участници“), в който се посочват причините за тяхното премахване. Износител на данни от ЕИП не може да разчита на РЗЛД за прехвърляне на лични данни на такива дружества. Имайте предвид, че компаниите, които са били извадени от списъка към Рамката за защита на личните данни, трябва

⁷ Обърнете внимание, че не всички самосертификации по РЗЛД обхващат данни за човешките ресурси. Следователно е важно да се провери дали това е така, ако е необходимо. Вж. също В3.

⁸ Вж. приложение I към решението за адекватност, принципи на рамката за защита на личните данни в отношенията между ЕС и САЩ, издадени от Министерството на търговията на САЩ, точка I.2.

⁹ Вж. определението за данни за ЧР във В1.

¹⁰ <https://www.dataprivacyframework.gov/list>

да продължат да прилагат принципите на Рамката по отношение на личните данни, получени по време на участието им в Рамката, докато съхраняват тези данни.

За предаването на лични данни на дружества в САЩ, които не са (или вече не са) самосертифицирани съгласно РЗЛД, може да се използват други основания за трансфер по глава V от ОРЗД, като например задължителни фирмени правила или стандартни договорни клаузи.

Фактът, че получателят в САЩ е самосертифициран съгласно РЗЛД, ще позволи на износителите на данни в ЕИП да спазват глава V от ОРЗД, но всички други изисквания в ОРЗД и всяко друго национално законодателство за защита на данните остават приложими.

3.1. Прехвърляне на данни на дъщерни предприятия на дружества в САЩ, сертифицирани съгласно Рамката за защита на личните данни в отношенията между ЕС и САЩ

В случай на прехвърляне на данни на дружества в САЩ, които са дъщерни предприятия на дружество майка, сертифицирано по РЗЛД, износителите на данни от ЕИП трябва да проверят дали сертификацията на дружеството майка обхваща и съответното дъщерно предприятие.

Можете да намерите допълнителна информация за това как да проверите обхвата на самосертификацията на дадена организация, включително дали тя обхваща и други американски структури или дъщерни предприятия в САЩ, [тук](#).¹¹

3.2. Предаване на данни на дружество в САЩ, действащо като администратор

Преди да предаде лични данни на администратор в САЩ, износител на данни от ЕИП трябва да гарантира, че предаването е в съответствие с всички разпоредби на ОРЗД. Като първа стъпка износителят на данни може да споделя лични данни с дружество в САЩ само ако има правно основание за обработката (член 6 от ОРЗД). Освен това трябва да бъдат изпълнени всички други изисквания в ОРЗД (напр. ограничение на целите, пропорционалност, точност и задължения за предоставяне на информация към субектите на данни). Следва да се отбележи, че когато данните трябва да бъдат предадени на самосертифицирано дружество в САЩ, износителят на данни от ЕИП, в съответствие с членове 13 и 14 от ОРЗД, трябва да информира субектите на данни относно получателите на техните данни и факта, че прехвърлянето попада в обхвата на решението за адекватност съгласно Рамката за защита на личните данни в отношенията между ЕС и САЩ.

3.3. Прехвърляне на дружество в САЩ, което действа като обработващ лични данни

Когато администратор от ЕИП прехвърля данни на обработващ лични данни в САЩ, администраторът и обработващият лични данни са задължени да сключат споразумение за обработване на данни съгласно член 28 от ОРЗД (по-нататък: споразумение за обработване на данни), независимо от това дали обработващият лични данни се е самосертифицирал съгласно РЗЛД.

¹¹[https://www.dataprivacyframework.gov/program-articles/How-to-Verify-an-Organization-s-Privacy-Data-Privacy-Framework-\(DPF\)-Commitments](https://www.dataprivacyframework.gov/program-articles/How-to-Verify-an-Organization-s-Privacy-Data-Privacy-Framework-(DPF)-Commitments)

Повече информация относно договорните изисквания за трансфер на лични данни към обработващ лични данни в САЩ можете да намерите [ТУК](#).¹²

Сключването на споразумение за обработване на данни е необходимо, за да се гарантира, че обработващият лични данни в САЩ се ангажира да:

- обработва личните данни само по документирано нареждане на администратора, включително що се отнася до предаването на лични данни на трета държава или международна организация, освен когато е длъжен да направи това по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни, като в този случай обработващият информира администратора за това правно изискване преди обработването, освен ако това право забранява такова информирание на основание наличие на важен обществен интерес;
- гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;
- прилага подходящи технически и организационни мерки, за да гарантира ниво на сигурност, съобразено с риска, в съответствие с изискванията на споразумението за обработване на данни (произтичащо от член 32 от ОРЗД) и раздели 4 и 10 от РЗЛД;
- спазва условията, посочени в споразумението за обработване на данни (произтичащи от член 28, параграфи 2 и 4 от ОРЗД) и раздел II.3.Б от РЗЛД за ангажиране на друг обработващ лични данни;
- взема предвид естеството на обработването, подпомага администратора, доколкото е възможно, чрез подходящи технически и организационни мерки при изпълнението на задължението на администратора да отговори на искания за упражняване на предвидените в глава III от ОРЗД права на субектите на данни;
- подпомага администратора да гарантира изпълнението на задълженията си съгласно членове 32—36 от ОРЗД, като отчита естеството на обработване и информацията, до която е осигурен достъп на обработващия лични данни;
- по избор на администратора заличава или връща на администратора всички лични данни след приключване на услугите по обработване и заличава съществуващите копия, освен ако правото на Съюза или правото на държава членка изисква тяхното съхранение;
- предоставя на администратора цялата информация, необходима за доказване на изпълнението на задълженията, определени в член 28 от ОРЗД, и позволява и допринася за извършването на одити, в т.ч. и проверки, от страна на администратора или друг одитор, оправомощен от администратора. Във връзка с тази последна точка обработващият лични данни незабавно информира администратора, ако по негово мнение дадено указание нарушава РЗЛД.

Когато обработващият лични данни в САЩ включва друг обработващ лични данни („обработващ лични данни подизпълнител“), за да извършва специфични дейности по обработването от

¹²<https://www.dataprivacyframework.gov/program-articles/Contract-Requirements-for-Data-Transfers-to-a-Processor>

името на администратора на лични данни от ЕИП, обработващият лични данни трябва да гарантира, че са изпълнени изискванията съгласно раздел II.3.B на РЗЛД. Това включва да се гарантира, че обработващият лични данни подизпълнител осигурява същото ниво на защита на личните данни, както се изисква в РЗЛД, и същите задължения за защита на данните, както е посочено в споразумението за обработване на данни. Когато обработващ лични данни подизпълнител не изпълни задължението си за защита на данните, първоначалният обработващ данните в САЩ продължава да носи пълна отговорност пред администратора за изпълнението на задълженията на този обработващ лични данни подизпълнител.

В4. КЪДЕ МОГА ДА НАМЕРЯ НАСОКИ ОТНОСНО СЕРТИФИЦИРАНЕТО НА АМЕРИКАНСКИ ДЪЩЕРНИ ПРЕДПРИЯТИЯ НА ЕВРОПЕЙСКИ ДРУЖЕСТВА?

Американските дъщерни предприятия на дружества от ЕИП могат да се самосертифицират съгласно РЗЛД, ако са под юрисдикцията на Федералната комисия по търговия (ФКТ) или на Министерството на транспорта на САЩ (МТ).

Можете да намерите повече информация относно изискванията за допустимост [ТУК](#)¹³, както и ръководство за процеса на самостоятелно сертифициране [ТУК](#).¹⁴

¹³[https://www.dataprivacyframework.gov/program-articles/U-S-Subsidiaries-of-European-Businesses-Participation-in-the-Data-Privacy-Framework-\(DPF\)-Program](https://www.dataprivacyframework.gov/program-articles/U-S-Subsidiaries-of-European-Businesses-Participation-in-the-Data-Privacy-Framework-(DPF)-Program)

¹⁴[https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-\(DPF\)-Program-\(part%E2%80%931\)](https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931))